



Kaseya 2

---

# Virtual System Administrator

---

**User Guide**

Version 6.1

July 7, 2011

**About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

# Contents

<b>Configuration</b>	<b>1</b>
Configuring the Server.....	3
System Security.....	3
Minimum System Requirements .....	3
Updating or Moving the VSA .....	3
Logon and Browser Settings .....	4
Creating Organizations Automatically During Update .....	6
<b>Getting Started</b>	<b>9</b>
VSA Modules.....	11
Page Layout .....	11
Toolbox.....	13
Status Monitor .....	13
Administrator Notes .....	14
Bookmarks.....	15
Logoff.....	15
Color Scheme .....	16
Agents.....	16
Check-in Icons.....	16
Live Connect.....	17
Data Table Column Options .....	18
Learning More .....	19
<b>Agent</b>	<b>21</b>
Agent Overview .....	23
Agents .....	24
Agent Icons .....	25
Machine ID / Machine Group Filter .....	26
View Definitions.....	28
Filter Aggregate Table .....	30
Advanced Filtering .....	30
Agent Status .....	31
Agent Logs .....	34
Log History .....	35
Event Log Settings .....	37
Deploy Agents .....	39
Agent Install Command Line Switches.....	44
Install Issues and Failures.....	45
Installing Multiple Agents .....	45
Installing Linux Agents .....	47
Supported Linux Functions .....	48
Supported Macintosh Functions.....	49
Create .....	49
Delete .....	53
Rename .....	54
Change Group.....	56
LAN Watch.....	56

Install Agents .....	60
View LAN .....	64
View AD Computers .....	65
View AD Users .....	66
View vPro.....	69
Copy Settings .....	70
Import / Export .....	71
Suspend.....	72
Agent Menu .....	73
Check-In Control.....	75
Working Directory .....	78
Edit Profile .....	79
Portal Access.....	81
Enabling Ticketing for Portal Access Users on Unsupported Browsers .....	82
Set Credential.....	83
Update Agent.....	84
File Access .....	85
Network Access.....	87
Application Blocker .....	89

---

## **Agent Procedures** **91**

Agent Procedures Overview.....	93
Schedule / Create .....	94
Agent Procedure Editor .....	96
IF-ELSE-STEP Commands.....	97
64-Bit Commands.....	114
Using Variables .....	115
Variable Manager .....	117
Manage Files Stored on Server .....	118
Folder Rights .....	119
Distribution.....	120
Agent Procedure Status .....	122
Patch Deploy .....	123
Application Deploy.....	124
Creating Silent Installs.....	125
Packager.....	127
Get File .....	127
Distribute File.....	129

---

## **Audit** **131**

Audit Overview .....	133
Run Audit.....	134
Audit Summary .....	135
Configure Column Sets .....	137
Machine Summary.....	137
System Info.....	140
Installed Applications.....	141
Add/Remove.....	142
Software Licenses .....	143
Documents .....	143

---

Inbox.....	147
Schedule.....	147
Reports.....	149
Report Definitions.....	149
Report Folder Trees.....	150
Publishing a Report Immediately.....	151
Scheduling a Report.....	151
Viewing Published Reports and Reports Set.....	152
Antivirus - Antivirus Installation Statistics.....	152
Anti-Malware - Anti-Malware Installation Statistics.....	153
Audit - Aggregate Table.....	153
Audit - Disk Utilization.....	153
Audit - Inventory.....	153
Audit - Machine Changes.....	154
Audit - Machine Summary.....	154
Audit - Network Statistics.....	155
Backup > Backup.....	156
Desktop Policy - Desktop Policy.....	156
Desktop Policy - Power Savings.....	156
Executive - Executive Summary.....	158
System Activity.....	159
Network Health Score.....	159
Logs - Logs.....	162
Logs - Admin Notes.....	163
Logs - Agent Log.....	163
Logs - Agent Procedure.....	163
Logs - Alarm Log.....	163
Logs - Configuration Changes.....	164
Logs - Event Logs.....	164
Logs - Event Logs Frequency.....	164
Logs - KES Log.....	165
Logs - Log Monitoring.....	165
Logs - Network Statistics Log.....	166
Logs - Remote Control.....	166
Monitoring - Monitor 95th Percentile.....	166
Monitoring - Monitor Action Log.....	167
Monitoring - Monitor Alarm Summary.....	167
Monitoring - Monitor Configuration.....	168
Monitoring - Monitor Log.....	168
Monitoring - Monitor Set.....	168
Monitoring - Monitor Trending.....	168
Monitoring - Uptime History.....	169
Patch - Patch Management.....	169
Security - Security.....	170
Service Desk - Custom Tickets.....	170
Service Desk - Service Goals.....	171
Service Desk - Service Hours.....	172
Service Desk - Service Times.....	172
Service Desk - Service Volumes.....	172
Service Desk - Tickets.....	173
Software - Software Applications Changed.....	173
Software - Software Applications Installed.....	174
Software - Software Licenses.....	174
Software - Software Licenses Summary.....	174

Software - Software Operating Systems .....	175
Ticketing - Customizable Ticketing .....	175
Ticketing - Ticketing .....	176
Time Tracking - Timesheet Summary .....	177
Time Tracking - Timesheet Entries .....	177
Reports Sets .....	177
Report Set Definitions .....	178
Report Set Folder Trees .....	178
Scheduling a Report Set .....	179
Customize .....	180
View Dashboard .....	180
Layout Dashboard .....	181

---

## **Monitor** **183**

Monitor Overview .....	185
Alarms .....	187
Dashboard List .....	189
Alarm List .....	191
Alarm Network Status .....	191
Alarm Summary Window .....	192
Alarm Rotator .....	193
Alarm Ticker .....	193
Network Status .....	193
Group Alarm Status .....	194
Monitoring Set Status .....	194
Machine Status .....	196
Device Status .....	196
Monitor Status .....	196
Machines Online .....	196
Top N - Monitor Alarm Chart .....	197
KES Status .....	197
KES Threats .....	197
Dashboard Settings .....	197
Alarm Summary .....	198
Suspend Alarms .....	199
Live Counter .....	201
Monitor Lists .....	202
Update Lists By Scan .....	203
Monitor Sets .....	204
Define Monitor Sets .....	206
Counter Thresholds .....	208
Services Check .....	210
Process Status .....	210
Monitor Icons .....	211
SNMP Sets .....	212
Define SNMP Set .....	213
SNMP Set Details .....	215
Add SNMP Object .....	217
SNMP Icons .....	218
Alerts .....	219
Alerts - Summary .....	220
Alerts - Agent Status .....	222
Alerts - Application Changes .....	225
Alerts - Get Files .....	227
Alerts - Hardware Changes .....	229

Alerts - Low Disk .....	232
Alerts - Event Logs .....	234
Edit Event Sets.....	239
Alerts - LAN Watch.....	240
Alerts - Agent Procedure Failure.....	243
Alerts - Protection Violation.....	245
Alerts - New Agent Installed.....	247
Alerts - Patch Alert .....	249
Alerts - Backup Alert.....	252
Alerts - System.....	256
SNMP Traps Alert.....	257
Assign Monitoring .....	261
Auto Learn - Monitor Sets .....	266
Monitor Log.....	267
System Check .....	269
LAN Watch.....	272
Assign SNMP .....	276
SNMP Quick Sets.....	281
Auto Learn - SNMP Sets.....	283
SNMP Log .....	284
Set SNMP Values .....	286
Set SNMP Type.....	287
Parser Summary.....	288
Log Parser .....	292
Log File Parser Definition .....	293
Assign Parser Sets .....	297
Log File Set Definition .....	301
Viewing Log Monitoring Entries .....	302

---

## **Patch Management** **303**

Patch Management Overview .....	305
Methods of Updating Patches .....	306
Configuring Patch Management.....	306
Patch Processing .....	307
Superseded Patches .....	307
Update Classification.....	308
Patch Failure .....	308
Scan Machine .....	310
Patch Status .....	312
Initial Update.....	313
Pre/Post Procedure: Patch Management.....	315
Automatic Update .....	317
Machine History.....	318
Machine Update .....	319
Patch Update.....	321
Rollback.....	324
Cancel Updates .....	325
Create/Delete: Patch Policy.....	326
Membership: Patch Policy .....	327
Approval by Policy .....	329
Approval by Patch .....	331
KB Override .....	333
Windows Auto Update .....	335
Reboot Action .....	337
File Source .....	340

Patch Alert .....	342
Office Source .....	346
Command Line .....	348
Patch Location .....	351

**Remote Control** **353**

---

Remote Control Overview .....	355
Control Machine .....	356
Video Streaming .....	359
Reset Password .....	360
Select Type.....	362
Set Parameters.....	363
Preinstall RC.....	364
Uninstall RC.....	366
User Role Policy .....	367
Machine Policy .....	368
FTP .....	370
Task Manager.....	372
Chat .....	373
Send Message.....	375
Power Management .....	377
Remote ISO Boot .....	378
Live Connect.....	380
Customized New Ticket Link.....	383

**System** **385**

---

System Overview.....	387
VSA Logon Policies.....	388
Embedding the VSA Logon Form in Web Pages.....	388
User Settings .....	391
Preferences .....	391
Change Logon.....	392
System Preferences .....	393
Check-in Policy.....	393
Naming Policy .....	395
User Security .....	397
Users .....	397
Master User vs. Standard Users.....	399
Create a New Master User .....	400
If Your Account Is Disabled.....	400
User Roles.....	400
Machine Roles.....	403
Scopes .....	404
Sharing User-Owned Objects .....	406
Logon Hours .....	407
User History.....	408
Orgs/Groups/Depts/Staff .....	408
Manage .....	408
Set-up Types .....	411
Server Management.....	412
Request Support .....	412
Configure.....	412
Processing Hotfixes Manually.....	417

Set URL to MS-SQL Reporting Services Engine.....	418
License Manager.....	420
Import Center .....	422
System Log .....	423
Statistics .....	423
Logon Policy.....	425
Application Logging.....	426
Outbound Email.....	426
Customize.....	428
Color Scheme.....	428
Site Customization .....	428
Creating Custom Agent Icons .....	430
Local Settings.....	431
Customize: Live Connect .....	432

---

**Ticketing** **433**

Ticketing Overview .....	435
View Summary .....	435
Create/View .....	438
Delete/Archive .....	441
Migrate Tickets .....	443
Notify Policy.....	443
Access Policy .....	445
Assignee Policy .....	446
Due Date Policy.....	447
Edit Fields.....	448
Email Reader.....	449
Email Mapping.....	451

---

**Time Tracking** **453**

Time Tracking Overview.....	455
Configuring Time Tracking .....	455
My Timesheets .....	457
Creating an Administrator Task Timesheet Entry .....	458
Creating a Customer / Work Order Timesheet Entry .....	458
Creating a Service Desk Ticket Timesheet Entry .....	458
Approve Timesheets.....	459
Timesheet Summary .....	460
Application Logging .....	460
Timesheet History (Summary).....	461
Timesheet History (Details) .....	461
Timers.....	461
Creating an Administrator Task Timer Entry.....	463
Creating a Customer / Work Order Timer Entry.....	463
Creating a Service Desk Ticket and Service Billing Timer Entry .....	464
Creating a Service Desk Ticket or Ticket/Task Timer Entry .....	465
Settings.....	466
Periods.....	466
Administrative Tasks .....	467
Approval Patterns .....	467

---

**Database Views** **469**

Database Views.....	472
Excel Usage .....	472
Crystal Reporting Usage .....	473
Views Provided.....	477
fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy .....	478
fnOSCounts .....	479
vAddRemoveList .....	480
vAdminNotesLog .....	480
vAgentConfiguration .....	480
vAgentLabel.....	482
vAlertLog.....	482
vBackupLog.....	483
vBaseApplicationInfo / vCurrApplicationInfo .....	484
vBaseCpuInfo / vCurrCpuInfo .....	485
vBaseDiskInfo / vCurrDiskInfo.....	485
vBaseDriveManufacturer / vCurrDriveManufacturer .....	486
vBasePciInfo / vCurrPciInfo.....	486
vBasePrinterInfo / vCurrPrinterInfo .....	487
vCollectionMember .....	487
vConfigLog .....	488
vkadComputers .....	488
vkadUsers.....	489
vLicenseInfo .....	489
vMachine .....	490
vMonitorAlarmAlert .....	492
vMonitorAlarmCounter.....	493
vMonitorAlarmProcess .....	494
vMonitorAlarmService .....	494
vMonitorAlarmSNMP .....	495
vMonitorAlarmSystemCheck .....	496
vNetStatsLog .....	497
vNtEventLog .....	497
vOnBoardDeviceInfo .....	498
vPatchApprovalStatus .....	498
vPatchConfiguration .....	499
vPatchPolicy .....	501
vPatchPolicyMember.....	502
vPatchStatus .....	502
vPortInfo .....	504
vScriptLog.....	505
vScriptStatus .....	505
vSystemInfo.....	506
vSystemInfoManual.....	507
vTicketField .....	507
vTicketNote.....	508
vTicketSummary.....	508
vUptimeHistory .....	509
vvProAssetDetails .....	509

---

**API Web Services** **511**

VSA API Web Service .....	513
VSA API Web Service - Overview.....	513
Enabling VSA API Web Service.....	514

Special Fields.....	514
VSA API Web Service Sample Client - C# GUI application .....	515
VSA API Web Service Sample Client - ASP Page .....	516
VSA API Web Service Security.....	519
Web Links - Inbound and Outbound .....	521
VSA API Web Service - Operations .....	522
AddMachGroupToScope.....	522
AddOrg .....	523
AddOrgDeptStaff.....	523
AddOrgToScope .....	523
AddScope.....	523
AddScopeOrg.....	524
AddTicRequest.....	524
AddUserToRole.....	524
AddUserToScope.....	524
AdminGroupAccess .....	525
AssignRole .....	525
AssignScope .....	525
Authenticate .....	525
AuthenticateWithAppSessionID .....	526
CloseAlarm.....	526
CreateAdmin .....	526
CreateAgentInstallPackage .....	527
CreateMachineGroup.....	527
CreateRole .....	527
DeleteAdmin.....	527
DeleteAgent .....	527
DeleteAgentInstallPackage.....	528
DeleteMachineGroup .....	528
DeleteOrg .....	528
DeleteRole .....	528
DeleteScope.....	529
DisableAdmin .....	529
Echo .....	529
EchoMt .....	529
EnableAdmin .....	529
GetAlarm .....	530
GetAlarmList .....	531
GetGroupLicenseInfo .....	531
GetLogEntry .....	532
GetMachine .....	532
GetMachineCollectionList .....	535
GetMachineGroupList .....	535
GetMachineList .....	535
GetMachineUptime .....	536
GetNotesList .....	536
GetOrgLocation.....	537
GetOrgs.....	537
GetOrgsByScopeID .....	537
GetOrgTypes.....	538
GetPackageURLs .....	538
GetPartnerUserLocation .....	538
GetPublishedViewColumns .....	539
GetPublishedViewRows.....	540
GetPublishedViews .....	541
GetRoles .....	544

GetScopes .....	544
GetSessionDetails .....	544
GetTicket.....	545
GetTicketList .....	546
GetTicketNotes .....	546
GetTicRequestTicket .....	547
GetVerboseMachineGroupList.....	547
LockFunctionAccess .....	547
Primitives.....	547
RemoveUserFromRole .....	549
ResetPassword .....	549
RoleMembership .....	549
SendAdminMessage.....	549
SetAdminPassword.....	550
SetGroupLicenseInfo .....	550
SetPartnerUserLocation.....	550
UpdateOrg.....	550
UpdateTicket.....	550
UpdateUser .....	552
Agent Procedure API Web Service .....	552
Enabling the Agent Procedure API Web Service.....	552
Agent Procedure API Web Service - Operations .....	552
AddScriptAssignment.....	553
AddScriptPrompt.....	553
Echo .....	553
EchoMt .....	553
GetScriptAssignmentId .....	553
GetScriptIdFromScriptName .....	554
Monitoring API Web Service.....	554
Enabling the Monitoring API Web Service .....	554
Monitoring API Web Service - Operations .....	554
AssignEventAlertToMachine .....	554
AssignEventLogMachineSettings .....	554
CreateEventSet.....	555
CreateEventSetDefinition.....	555
DeleteAllEventAlertsFromMachine .....	555
DeleteAllEventLogMachineSettings.....	555
DeleteEventAlertFromMachine .....	556
DeleteEventLogMachineSettings.....	556
DeleteEventSet .....	556
DeleteEventSetDefinition .....	556
GetEventAlertList .....	556
GetEventLogMachineSettingsList.....	557
GetEventSetDefinitionList .....	558
GetEventSetList .....	558
KSD API Web Service .....	559
Enabling KSD API Web Service.....	559
KSD API Web Service Data Types .....	559
RefItem.....	559
CustomField .....	560
Note.....	560
Attachment .....	560
RelatedIncident .....	560
ServiceDeskDefinition .....	561
Incident Summary .....	563
Incident.....	564

KSD API Web Service - Operations.....	566
AddIncident .....	566
AddServDeskToScope.....	566
GetIncident.....	566
GetIncidentList.....	567
GetServiceDesk.....	568
GetServiceDesks.....	568
Primitives.....	569
UpdateIncident.....	569
Sample Messages.....	569
GetServiceDesks Request.....	569
GetServiceDesks Response.....	569
GetServiceDesk Request.....	570
GetServiceDesk Response.....	570
GetIncidentList Request.....	577
GetIncidentList Response.....	577
GetIncident Request.....	577
GetIncident Response.....	577
AddIncident Request.....	579
AddIncident Response.....	579
UpdateIncident Request.....	579
UpdateIncident Response.....	581

---

Active Directory .....	583
Agent Menu .....	583
Agent Quick View Window .....	583
Agent Settings .....	583
Agents.....	584
Agents - Linux.....	584
Agents - Macintosh.....	584
Alarm .....	585
Alarm Condition .....	585
Alarms - Suspending .....	585
Alert .....	585
Alert Types .....	586
ATSE Response Code .....	587
Audit.....	587
Auto Learn Monitor Sets.....	587
Backup Sets .....	587
Canonical Name .....	587
Chat .....	587
Check-in Status .....	588
Check-in: Full vs. Quick.....	588
Collection.....	588
Copy Settings and Templates .....	588
Credential .....	588
Current VSA Time .....	589
Dashboard .....	589
Dashboard List .....	589
Distribute File.....	589
Event Logs.....	589
Events Sets .....	590
File Transfer Protocol (FTP).....	590
Flood Detection .....	590
Global Event Log Black Lists.....	590
Group Alarms .....	590
Host name .....	590
Hotfix.....	590
ISO Image .....	591
LAN Watch .....	591
Log Monitoring.....	591
Logs .....	591
MAC address.....	592
Machine ID / Group ID / Organization ID.....	592
Machine ID / Group ID filter .....	592
Machine ID Template .....	592
Machine IDs vs. Agents.....	592
Machine Roles.....	593
Managed Machine .....	593
Master User / Standard User.....	593
Migrating the KServer.....	593
Monitor Sets .....	593
Monitor Types .....	594
myOrg .....	594
Org.....	594
Packager .....	594
Parser Definitions and Parser Sets .....	595

Patch Policy .....	595
Patch Update Order.....	595
Performance Objects, Instances and Counters .....	596
Portal Access.....	596
Primary Domain Controller .....	596
Private Folders .....	596
Quick Status .....	597
Silent Install .....	597
SNMP Community.....	597
SNMP Devices .....	597
SNMP Quick Sets.....	597
SNMP Sets .....	598
SNMP Types .....	598
Software as a Service (SaaS) .....	599
syslog.....	599
System Agent Procedures.....	599
System Checks.....	599
System Tray .....	599
User Account .....	600
Users .....	600
View Definitions .....	600
Virtual Machine.....	600
Virtual Network Computing (VNC).....	600
vPro .....	600
Windows Automatic Update .....	600
Work Types .....	600



## Chapter 1

# Configuration

### In This Chapter

Configuring the Server	3
System Security	3
Minimum System Requirements	3
Updating or Moving the VSA	3
Logon and Browser Settings	4
Creating Organizations Automatically During Update	6

## **Configuration**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

## Configuring the Server

The server is the heart of the system. Users access all functions through this server's web interface. The agents, on all managed machines, connect to this server to get any instructions/tasking orders. Your server must be accessible to both users and agents.

For configuring the server, see the latest [Installation Guide](#) install at [http://help.kaseya.com/WebHelp/en/VSA/6010000/EN\\_KServerInstallation61.pdf](http://help.kaseya.com/WebHelp/en/VSA/6010000/EN_KServerInstallation61.pdf).

The [Kaseya SSRS Configuration](#) guide is a companion document that provides additional guidance on integrating SQL Services Reporting Services with Kaseya, located at [http://help.kaseya.com/WebHelp/en/VSA/6010000/EN\\_SSRSguide61.pdf](http://help.kaseya.com/WebHelp/en/VSA/6010000/EN_SSRSguide61.pdf).

---

## System Security

We designed the system with comprehensive security throughout. Our design team brings over 50 years of experience designing secure systems for government and commercial applications. We applied this experience to uniquely combine ease of use with high security.

The platform's architecture is central to providing maximum security. The agent initiates all communications back to the server. Since the agent will *not* accept any inbound connections, it is virtually impossible for a third party application to attack the agent from the network. *The system does not need any input ports opened* on the managed machines. This lets the agent do its job in virtually any network configuration without introducing any susceptibility to inbound port probes or new network attacks.

The VSA protects against man-in-the-middle attacks by encrypting all communications between the agent and server with 256-bit RC4 using a key that rolls every time the server tasks the agent. Typically at least once per day. Since there are no plain-text data packets passing over the network, there is nothing available for an attacker to exploit.

Users access the VSA through a web interface after a secure logon process. The system never sends passwords over the network and never stores them in the database. Only each user knows his or her password. The client side combines the password with a random challenge, issued by the VSA server for each session, and hashes it with SHA-1. The server side tests this result to grant access or not. The unique random challenge protects against a man-in-the-middle attack sniffing the network, capturing the random bits, and using them later to access the VSA.

The web site itself is protected by running the Hotfix Checker tool on the VSA server every day. The VSA sends alerts to the `Master` role user when new IIS patches are available. This helps you keep the VSA web server up to the latest patch level with a minimum of effort. Finally, for maximum web security, the VSA web pages fully support operating as an SSL web site.

---

## Minimum System Requirements

Up to date minimum system requirements are available at: <http://help.kaseya.com/WebHelp/en/system-requirements.asp>.

---

## Updating or Moving the VSA

If you are updating from an earlier version of Kaseya to this version, or want to update or move your existing K2 server to the latest version, see the installation guide at [http://help.kaseya.com/WebHelp/en/VSA/6010000/EN\\_KServerInstallation61.pdf](http://help.kaseya.com/WebHelp/en/VSA/6010000/EN_KServerInstallation61.pdf).

---

## Logon and Browser Settings

### To logon to Virtual System Administrator™

1. Use your browser to display the logon page of your VSA server.
2. Enter your user name and password.

**Note:** For initial logon, use the master user account name and password entered during installation.

3. Check the **Remember my username and domain (if any) on this computer** checkbox to save the username and domain name to a cookie on the local computer so you don't have to re-enter each time you log in. The password is not stored.

**Note:** See [System > Change Logon](#) (page 392) for a description of how to set up a domain logon.

4. Click the **logon** icon .

**Note:** To prevent unauthorized access after making configuration changes, log off or close the session by terminating the browser application.

### Enabling Browser Cookies, JavaScript and Popups

Your browser must have cookies and JavaScript enabled in order to proceed. Popups for the VSA website are recommended.

#### Internet Explorer

##### To Enable Cookies in Internet Explorer 7 or 8

1. Click the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Privacy** tab.
4. Select a privacy setting no greater than **Medium High** (i.e. the setting must not be High nor Block All Cookies).
5. Click **OK**.

##### To Enable JavaScript in Internet Explorer 7 and 8

1. Click on the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Security** tab.
4. Click on **Internet** in the **Select a Web** content zone.
5. Press the **Custom level...** button.
6. Scroll down to the **Scripting** section.
7. In **Scripting of Java applets**, click the **Enable** option.
8. Click **OK**.

##### To Enable Popups in Internet Explorer 7 or 8

1. Click the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Privacy** tab.
4. Click **Settings**. The Pop-up Blocker Settings dialog displays.

5. Enter the URL or IP address of your VSA in the **Address of website to allow** field.
6. Click **Close**, then **OK**.

## **Firefox**

### *To Enable Cookies in Firefox*

1. Click the **Tools** menu.
2. Select **Options**.
3. Switch to **Privacy** settings.
4. Set History to **Remember History**. (You can also **Use custom settings for history** and make sure **Accept cookies from site** is checked.)
5. Click **OK**.

### *To Enable JavaScript in Firefox*

1. Click on the **Tools** menu.
2. Select **Options**.
3. Switch to the **Content** tab.
4. Click the **Enable Java** checkbox.
5. Click **OK**.

### *To Enable Popups in Firefox*

1. Click on the **Tools** menu.
2. Select **Options**.
3. Switch to the **Content** tab.
4. Click **Exceptions...** The **Allowed Sights - Pop-ups** dialog displays.
5. Enter the URL or IP address of your VSA in the **Address of web site** field.
6. Click **Allow**.
7. Click **Close**, then **OK**.

## **Chrome**

### *To Enable Cookies in Chrome*

1. Click the **Tools** icon.
2. Select **Options**.
3. Select the **Under the Hood** tab.
4. Switch to **Content settings...**
5. Select the **Cookies** feature.
6. Select the **Allow local data to be set (recommended)** option.
7. Click **OK**.

### *To Enable JavaScript in Chrome*

1. Click the **Tools** icon.
2. Select **Options**.
3. Select the **Under the Hood** tab.
4. Switch to **Content settings...**
5. Select the **JavaScript** feature.
6. Select the **Allow all site sites to run JavaScript (recommended)** option.

## Configuration

7. Click **OK**.

### To Enable Popups in Chrome

1. Click the **Tools** icon.
2. Select **Options**.
3. Select the **Under the Hood** tab.
4. Switch to **Content settings...**
5. Select the **Pop-ups** feature.
6. Select the **Do not allow any site sites to show pop-ups (recommended)** option.
7. Click **Exceptions...** The **Pop-up Exceptions** dialog displays.
8. Click **Add...** the **New Exception** dialog displays.
9. Enter the URL or IP address of your VSA.
10. Set **Action** to **Allow**.
11. Click **OK**, then **Close** for all the parent dialogs.

---

## Creating Organizations Automatically During Update

Kaseya 2 introduces **organizations** to the machine group hierarchy that did not exist in earlier versions of the VSA. Each machine group must belong to an **organization**. During an update of Kaseya 2 from a 5.1 or earlier version, or during a restore of Kaseya 2, you are asked to decide how organizations should be created for machine groups.

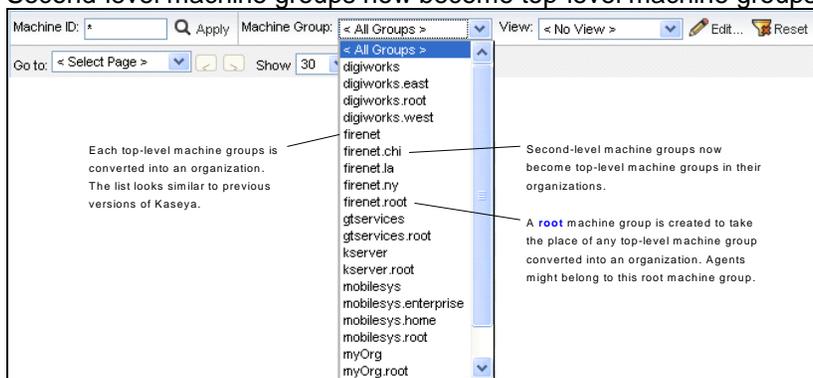
*This question is asked when you are:*

- You are upgrading from Kaseya 5.1 or earlier.
- You previously installed a new VSA and click the **Restore** button on the **System > Configure** page to restore a database from Kaseya version 5.1 or earlier.

### Create Multiple Organizations, One for Each Top-Level Machine Group

*Use this option if most of your existing machine groups represent external customers.*

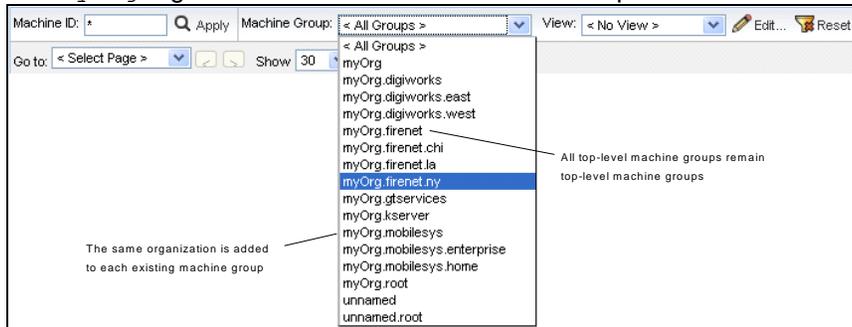
- Each top-level machine group is converted into its own organization.
- Machine group listings appear similar to the way they looked in earlier versions of the VSA.
- A special `root` machine group is created to take the place of a top-level machine group converted into an organization. The `root` machine group contains any agents that belonged to the top-level machine group converted into an organization.
- Second-level machine groups now become top-level machine groups in the new organization.



### Create a Single Organization

Use this option if most of your existing machine groups belong to the same organization.

- All machine groups are added to a single *myOrg* organization, representing your own organization.
- The *myOrg* organization can be renamed after the update.





## Chapter 2

# Getting Started

### In This Chapter

VSA Modules	11
Page Layout	11
Toolbox	13
Status Monitor	13
Administrator Notes	14
Bookmarks	15
Logoff	15
Color Scheme	16
Agents	16
Check-in Icons	16
Live Connect	17
Data Table Column Options	18
Learning More	19

## **Getting Started**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

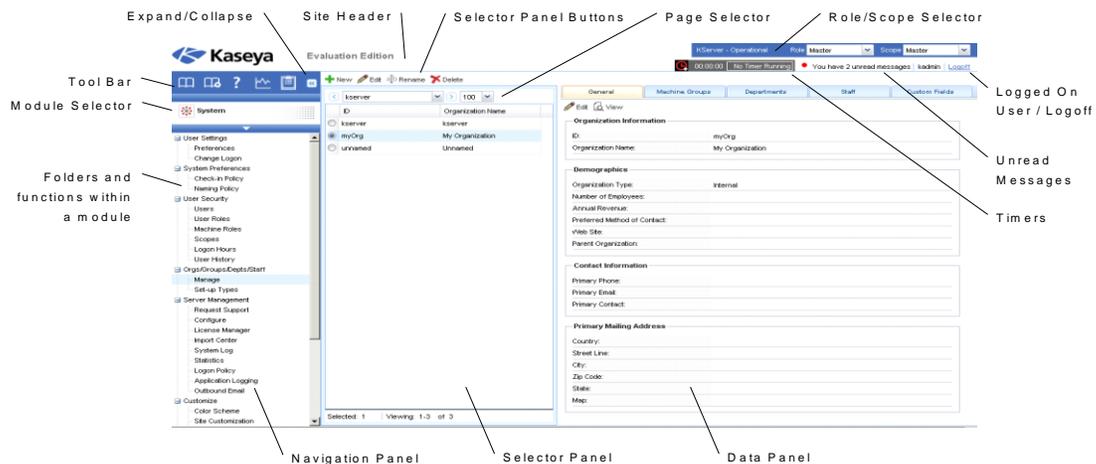
# VSA Modules

All VSA functions can be accessed through modules located along the left side of the user interface. Within each module are the core functions that allow users to perform a variety of tasks on remotely managed machines and the KServer.



# Page Layout

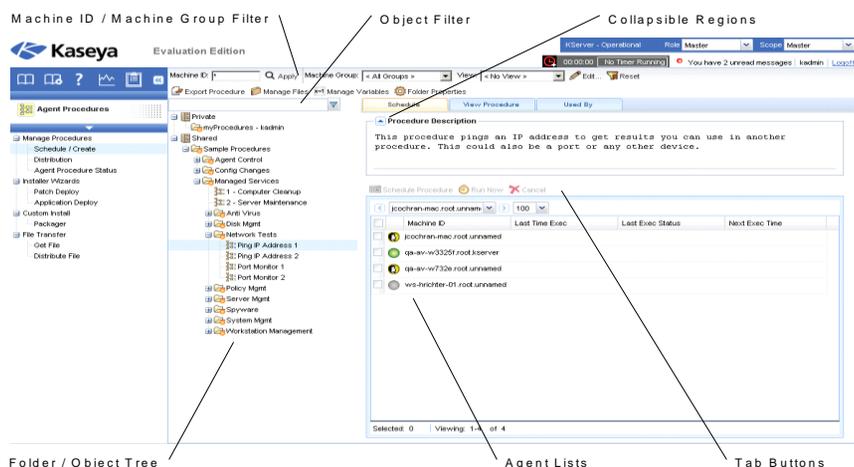
The user interface of Kaseya 2 is designed to be flexible while streamlining the choices a user makes.



- **Navigation Panel** - The module tabs and function panes are combined into a single expandible-collapsible explorer like navigation panel.
- **Selector Panel** - Many Kaseya 2 functions display a middle selector panel to select one or more records. The selector panel can be scrolled, filtered and sorted independently from any other pane.

## Getting Started

- **Data Panel** - On the right hand side of the screen, is a data panel designed as a series of tabbed views, providing quick access to each property or data view no matter how complex a function might be. Many of the tabs have fields you can edit and buttons that provide additional functionality.
- **Module Selector** - At the top of the navigation panel is a module selector. Clicking the visible module displays all the installed modules in the VSA. Clicking any of the other modules selects that module and displays the folders and functions within that module the user has access rights to see.
- **Toolbar** - The toolbar, just above the module selector, provides instant access to the global functions **Show Bookmarks**, **Add Bookmark**, **Help**, **Status**, and **Notes**.
- **Expand/Collapse** - A << icon on the right side of the toolbar collapses the navigation panel. Once collapsed a >> icon expands the navigation panel.
- **Selector Panel Buttons** - At the top of the selector panel is a page-specific button bar. Typically these buttons include creating, editing and deleting records listed in the selector panel. Additional buttons display, depending on the page and your logon access rights.
- **Page Selector** - If the selector panel list is longer than one page, the page selector enables you to browse through multiple pages. You can set the number of rows displayed on each page.
- **Site Header** - A customizable site logo and header text displays in the upper left corner.
- **Role/Scope Selector** - Selects the combination of role and scope that is currently active for your logon. If you have more than one role or scope available to you, you can switch roles or scopes anytime during your logon.
- **Logged On User / Logoff** - Displays the username of the user currently logged on and a logoff link.
- **Unread Messages** - The number of unread messages displays in the upper right corner. You can click this counter at any time to display your VSA inbox immediately.
- **Timers** - Records time entries that can be applied to timesheets and other work type records.



- **Machine ID / Machine Group Filter** - If a page displays an agent list, then the Machine ID / Machine Group filter displays at the top of the page. The filter enables you to limit the list of agents displayed on the machine, by individual machine, machine group, organization or by view definition.
- **Folder / Object Trees** - Certain functions display a folder tree in the selector panel instead of list of records. Typically two folder trees are provided, one **Private** and one **Shared**, but sometimes only the Shared folder tree displays. You can create new objects in these folder trees, and in the **Shared** folder tree, share them with other users.
- **Tree Filter** - All folder trees panels can be filtered by entering a string into the tree filter.
- **Agent Lists** - Agents lists display on many VSA pages. In the new user interface, agents frequently display in one of the tabs in the data panel on the right side of the page.
- **Tab Specific Buttons** - Any tab in the data panel on the right side of the page can display a tab specific set of buttons. Tab specific buttons affect the child record just below it. For example,

when you want to run an agent procedure immediately, you select the procedure in the folder tree in the middle panel, then select one or more of the agents in the tab, then click the "Run Now" tab button to execute the agent procedure.

- **Collapsible Regions** - Panels, tabs and dialogs are sometimes segmented into collapsible regions. Clicking the down arrow lets you hide that region of the user interface. A collapsed region displays an expand button, enabling you to expand that region again.

---

## Toolbox



The **Toolbox** provides the user with a common area to access frequently used commands and functions. The **Toolbox** is accessible from any module, giving users convenient access to frequently used features of the VSA.

### Notes

Click the **Notes** icon  to display the **User Notes** (*page 14*) window. **User Notes** provides a place to record and retrieve what previous user actions were performed on each machine.

### Status

Click the **Status** icon  to display the **Status Monitor** (*page 13*) window. **Status Monitor** continuously monitors selected machines, notifying you when they go online or offline.

### Help

Click the **Help** icon  to display context-sensitive help for the currently selected function page.

---

## Status Monitor

**Toolbox** > **Status**

The status monitor  continuously monitors selected machines, notifying you when they go online or offline. If someone is currently logged onto the machine, **Status Monitor** displays their user name in bold along with the IP address of the machine. Master role users can also display the list of logged on VSA users.

### Turn off sound

A unique audible tone sounds each time a machine goes online, machine goes offline, a user logs in, or a user logs out. Turn these sounds off by checking this box.

### Refresh Rate

Refreshes the browser every 30 sec, 1, 2, or 5 minutes. Each browser refresh gets the latest status from **Virtual System Administrator™**. To get an immediate update, click the **Refresh** link.

### List logged on users

Uncheck this box to hide the list of users.

Note: This option is available to master role users only.

### Sort By

List machines in any of the following order:

- **Connection Gateway** - Numerically, left to right, by IP address. Best for grouping machines by how they are connected on the network.
- **Group ID** - Alphabetically by group ID.
- **Machine ID** - Alphabetically by machine ID.

### Hide offline machines

Uncheck this box to list all machines. Offline machines have a grayed out icon.

---

## Administrator Notes

**Administrator Notes** allows you to log what you did to a machine or group of machines into the system database. The next time you have a problem with any machine, check the notes and see what other VSA users have done on that machine. The system time-stamps each administrator note and associates the note with a VSA user name.

Open the notes editor by clicking the Notes icon  in the **Toolbox** (page 13).

Note: You can print Administrator Notes using Info Center > Reports > Logs - Admin Notes (page 163).

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404). Check the box in front of the machines you wish to apply the note to.

### Time

Displays the time-stamp when the note was first entered. The time-stamp can be edited by clicking the edit icon  next to the specific note whose time-stamp you wish to change.

### Admin

Logon name of the user that entered the note. If a different user edits the note, this field is updated with the new user's name.

### Delete the note

Delete the note by clicking the delete icon  next to it. If more than one machine has the same note entered by the same user and has the same time-stamp, the system asks if you want to delete all occurrences of the note.

### Edit the note

Change a note by clicking the edit icon  next to it. Click the **Apply** button to commit the changes. Click **Cancel** to restore the original text. If more than one machine has the same note entered by the same user and has the same time-stamp, the system asks if you want to modify all occurrences of the note.

## Note

Displays the user entered note for the selected machine.

## Notes per Page

Number of notes to display at a time. Choices are 10, 30, and 100.

---

# Bookmarks



You can bookmark any item on the navigation pane. Bookmarks are defined by user. If you work with the same set of navigation items each day, this can save you navigation clicks.



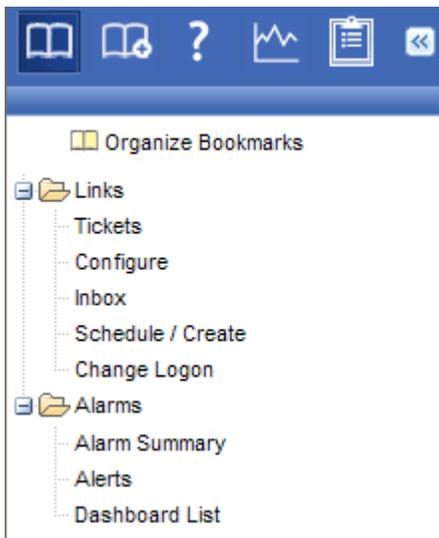
- Click the **Add Bookmark** icon to add a navigation item to your list of bookmarks.



- Click the **Bookmark Show** icon to display the list of bookmarks you have saved.



- Click the **Organize Bookmarks** icon in the bookmark list to create bookmark folders and organize your bookmarks.



---

# Logoff

Click the **Log Off** link to prevent unauthorized access to the server and return to the logon page. The **Log Off** link is located in the upper right-hand corner of the window and is accessible from any tab and function.

**Note:** For increased security, it is recommended that users log off and terminate all browser sessions when not administering the server.

---

## Color Scheme

### System > Color Scheme

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Color Scheme** page determines the set of colors displayed by the VSA environment. **Color Scheme** selection is by user and persists between logon sessions.

To change color schemes:

1. Select a color scheme in the middle pane.
2. Click the **Set Scheme** button.

---

## Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the  agent icon—displays in the system tray of the managed machine. **Agent icons** (page 25) can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** (page 592). Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > **Deploy Agents** (page 39) inside the VSA.
- **Multiple agents** (page 45) can be installed on the same machine, each pointing to a different server.
- A **check-in icon** (page 16) displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the  check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called **Live Connect** (page 17). **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an **agent quick view window** (page 583) immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

---

## Check-in Icons

Once a machine ID is created, an agent check-in icon displays next to each machine ID account in the VSA. These icons indicate the agent check-in status of each managed machine. Click a check-in icon to display **Live Connect** (page 17). Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on. Icon displays a tool tip showing the logon name.

-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Live Connect

The **Live Connect** page displays by *clicking* any check-in icon, for example , next to any machine ID in the VSA. **Live Connect** enables you to perform tasks and functions solely for one managed machine. A menu of tabbed property sheets provide access to various categories of information about the managed machine.



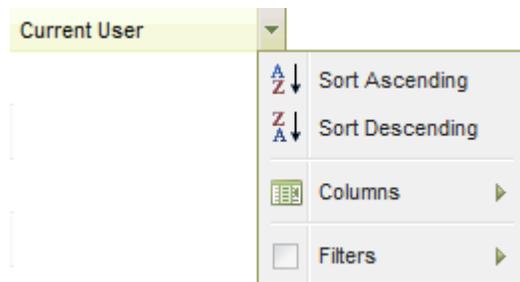
- **Home** - The first view displayed when the Live Connect window opens. *You can customize the Live Connect Home page using System > Customize: Live Connect (page 432).*
- **Agent Data** - Displays agent data and initiates agent tasks on the managed machine.
- **Audit Information** - Displays the software and hardware configuration of the managed machine.
- **File Manager** - Provides two file managers, one for your local machine and one for the remote machine ID, enabling you to browse and transfer files between the two machines.
- **Command Shell** - Opens a command shell into the managed machine.
- **Registry Editor** - Displays the registry of the managed machine ID. You can create, rename, refresh or delete keys and values and set the data for values.
- **Task Manager** - Lists Task Manager data for the managed machine.
- **Event Viewer** - Displays event data stored on the managed machine.
- **Ticketing** - Displays and creates tickets for the managed machine.
- **Chat** - Initiates a chat session with the currently logged on user of the managed machine.
- **Desktop Access** - Initiates a remote desktop session with the managed machine.
- **Anti-Malware** - Displays the Anti-Malware status of the managed machine, if installed.
- **Anti-Virus** - Displays the Antivirus status of the managed machine, if installed.
- **Discovery** - Displays the Network Discovery status of the machine, if installed.
- **Video Chat** - Initiates a audio/video chat session with a logged on machine user.

This same **Live Connect** window displays when a machine user clicks the  agent icon in the system tray of the managed machine, with certain restrictions applied. This machine user view of **Live Connect** is called **Portal Access**.

**Note:** For more details, see [Remote Control > Live Connect \(page 380\)](#).

## Data Table Column Options

Data tables in Kaseya 2 typically provide the following column options.



- **Column Selection** - Click any column header drop-down arrow  , then **Columns** to select which columns display in the table. Click the Sort Ascending  or Sort Descending  icons to sort the table by the selected column heading.
- **Column Sorting** - Click the Sort Ascending  or Sort Descending  icons to sort the table by the selected column heading.
- **Column Filtering** - Click the column drop-down arrow  to enter a filter value for that column. For example enter `NS` to find all rows that start with `NS` in that column. Enter `NS%2` to find all rows that start with `NS` and end with `2` in that column. You can filter by multiple column filters if you like.
- **Flexible Column Widths** - Expand or collapse the width of each column by dragging the column header boundaries left or right.

---

## Learning More

PDFs are available to help you quickstart your implementation of **Virtual System Administrator™**. They can be downloaded from the **first topic in online help** (<http://help.kaseya.com/WebHelp/EN/VSA/6010000/index.htm?toc.htm?6939.htm>).

If you're new to **Virtual System Administrator™** we recommend the following quickstart guides:

1. Getting Started
2. User Administration
3. Agent Configuration and Deployment
4. Live Connect and Portal Access
5. Monitoring Configuration

The following resources are also available.

### Training

---

You can view VSA training videos at the **Kaseya Portal** (<http://portal.kaseya.net>). Click the *Kaseya LMS* link under the Education folder.

---



## Chapter 3

# Agent

### In This Chapter

Agent Overview	23
Agent Status	31
Agent Logs	34
Log History	35
Event Log Settings	37
Deploy Agents	39
Create	49
Delete	53
Rename	54
Change Group	56
LAN Watch	56
Install Agents	60
View LAN	64
View AD Computers	65
View AD Users	66
View vPro	69
Copy Settings	70
Import / Export	71
Suspend	72
Agent Menu	73
Check-In Control	75
Working Directory	78
Edit Profile	79
Portal Access	81
Set Credential	83
Update Agent	84
File Access	85
Network Access	87
Application Blocker	89

## **Agent**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Agent Overview

## Agent

Functions in the **Agent** module allow users to create, edit, and delete machine IDs, customize the appearance of the machine's agent icon  in the **system tray** (on page 599), control agent check-in frequency, and update the version of agent software that resides on managed machines.

**Note:** You can download an [Agent Configuration and Deployment PDF](#) from the first topic of online help.

Functions	Description
<a href="#">Agent Status</a> (page 31)	Displays active user accounts, IP addresses and last check-in times.
<a href="#">Agent Logs</a> (page 34)	Displays logs of: <ul style="list-style-type: none"><li>• Agent system and error messages</li><li>• Execution of agent procedures, whether successful or failed.</li><li>• Configuration changes made by a user.</li><li>• Send/receive data for applications that access the network.</li><li>• Application, System, and Security event log data collected from managed machine.</li><li>• Alarm log</li><li>• Remote control log</li><li>• Log monitoring</li></ul>
<a href="#">Log History</a> (page 35)	Specifies how long to store log data.
<a href="#">Event Log Settings</a> (page 35)	Specifies event log types and categories included in event logs.
<a href="#">Deploy Agents</a> (page 39)	Creates agent install packages for installing agents on multiple machines.
<a href="#">Create</a> (page 49)	Creates machine ID accounts and/or install packages for installing agents on single machines.
<a href="#">Delete</a> (page 53)	Deletes machine ID accounts.
<a href="#">Rename</a> (page 54)	Renames existing machine ID accounts.
<a href="#">Change Group</a> (page 56)	Reassigns machines to a different machine group or subgroup.
<a href="#">LAN Watch</a> (page 56)	Uses an existing agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran.
<a href="#">Install Agents</a> (page 60)	Installs the agent <i>on a remote system</i> and creates a new machine ID / group ID account for any new PC detected by LAN Watch.
<a href="#">View LAN</a> (page 64)	Displays the results of the latest LAN Watch scan.
<a href="#">View AD Computers</a> (page 65)	Lists all computers listed in an Active Directory when LAN Watch runs on a system hosting Active Directory. Installs agents on AD machines.
<a href="#">View AD Users</a> (page 66)	Lists all Active Directory users discovered by LAN Watch when LAN Watch runs on a system hosting Active

## Agent

	Directory. Creates VSA users from AD users.
<b>View vPro</b> (page 69)	Displays hardware information about vPro-enabled machines discovered while running LAN Watch.
<b>Copy Settings</b> (page 70)	Mass copies settings from one machine account to other machine accounts.
<b>Import / Export</b> (page 71)	Imports and exports agent settings, including scheduled agent procedures, assigned monitor sets, and event sets, as XML files.
<b>Suspend</b> (page 72)	Suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings.
<b>Agent Menu</b> (page 73)	Customizes the agent menu on managed machines.
<b>Check-In Control</b> (page 75)	Controls agent check-in frequency on agent machines.
<b>Working Directory</b> (page 78)	Sets the path to a directory used by the agent to store working files.
<b>Edit Profile</b> (page 79)	Edits machine account information.
<b>Portal Access</b> (page 81)	Sets up accounts to allow machine users remote control access to their own machines.
<b>Set Credential</b> (page 83)	Sets a logon credential for the agent to use in Patch Management, the Use Credential procedure command, Endpoint Security, and Desktop Policy and Migration.
<b>Update Agent</b> (page 84)	Updates the agent software on managed machines.
<b>File Access</b> (page 85)	Prevents unauthorized access to files on managed machines by rogue applications or users.
<b>Network Access</b> (page 87)	Lets you approve or deny network access on a per application basis.
<b>Application Blocker</b> (page 89)	Application blocker prevents any application from running on a managed machine.

## Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the  agent icon—displays in the system tray of the managed machine. **Agent icons** (page 25) can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** (page 592). Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > **Deploy Agents** (page 39) inside the VSA.
- **Multiple agents** (page 45) can be installed on the same machine, each pointing to a different server.
- A **check-in icon** (page 16) displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the  check-in icon indicates an agent is online and the user is currently logged on.

- Clicking a check-in icon displays a single machine interface for the managed machine called **Live Connect** (page 17). **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an **agent quick view window** (page 583) immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

## Agent Icons

Once installed on a machine, the agent displays an icon in the computer's system tray. This icon is the machine user's interface to the agent. The icon may be disabled at the discretion of the VSA user using the Agent > **Agent Menu** (page 73) page.

**Note:** You can fully customize agents icon using System > Site Customization. See **Creating Custom Agent Icons** (page 430). This includes unique icons for Macintosh and Linux machines.

### Agent Icon Background is Blue

When the agent is running and **successfully checking into the VSA**, the agent icon's background is **blue**.



**Note:** Double clicking the agent icon displays the **Portal Access Welcome Page** (page 596).

### Agent Icon Background is Grey

A running agent that can **not** check into the VSA displays a **gray icon**. This indicates that either the network connection is down or the agent is pointed at the wrong address for the VSA.



If the agent icon is gray check the following:

1. Verify this machine has internet access.
2. Check to see if there is a firewall blocking the **outbound** port used by the agent to connect to the VSA. The default is port 5721.
3. Verify this machine account's **Check-in Control** (page 75) settings are correct.
4. Manually set the VSA server address in the agent by right clicking the agent menu, selecting **Set Account...**, and filling in the form with the correct address.

### Set Agent Account Information ✕

Please enter the address of your management server. This Agent automatically connects to the server's IP Address or hostname to manage your system.

Machine.Group ID

Server Address

## Agent

### Agent Icon Background is Red

The agent icon turns **red** when a machine user manually disables remote control. VSA users prevent anyone from remote controlling their machine by selecting **Disable Remote Control** when they right click the agent menu.



### Agent Icon Background Flashes between White and Blue

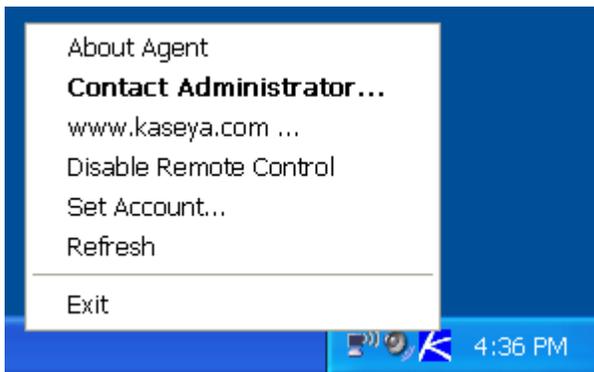
The agent icon **flashes** between a white background and its normal background when a *message is waiting* to be read. Clicking the icon displays the message.



**Note:** See [Remote Control > Send Message \(page 375\)](#) for an explanation of how to set up the sending of messages.

### Agent Menu Options

Right clicking the agent icon pops up a menu of options available to the machine user.



**Note:** See [Agent > Agent Menu \(page 73\)](#) for a description of how to turn these options on or off.

### Disabling the Agent Menu

VSA users may completely **disable the agent menu** ([page 73](#)) and remove the icon from the machine's desktop.



## Machine ID / Machine Group Filter

### Machine ID / Machine Group Filter

Each **agent** ([page 583](#)) installed on a managed machine is assigned a unique **machine ID / group ID / organization ID**. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all the machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.sales.chicago.acme`. In this case `sales` is a subgroup ID

within the `chicago` group ID within the organization ID called `acme`. In some places in the VSA, this hierarchy is displayed in reverse order. Each organization ID has a single default machine group ID called `root`. Group IDs and subgroup IDs are created using the System > Orgs/Group/Depts/Staff > Manage > **Machine Groups** (page 410) page.

## Filtering Views



The screenshot shows a filtering interface with the following elements: a 'Machine ID' input field with a search icon and an 'Apply' button; a 'Machine Group' dropdown menu set to '< All Groups >'; a 'View' dropdown menu set to '< No View >'; an 'Edit...' button with a pencil icon; and a 'Reset' button with a trash icon. Below these is a 'Go to' field containing 'aegisw02.aegis.at', navigation arrows, a 'Show' dropdown set to '10', and a machine count of '1084 machines'.

The Machine ID / Machine Group filter is available on all tabs and functions. It allows *you* to limit the machines displayed on *all* function pages. The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. Once filter parameters are specified, click the **Apply** button to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in <All Groups> managed by the currently logged on VSA user.

**Note:** Even if a VSA user selects <All Groups>, only groups the VSA user is granted access to using System > User Security > **Scopes** (page 404) are displayed.

## Machine ID

Limits the display of data on *all* function pages by machine ID string. Include an asterisk (\*) wildcard with the text you enter to match multiple records. For example, entering the string `ABC*` limits the display of machine IDs on all function pages to machine IDs that start with the letters `ABC`.

## Apply

Click the **Apply** button to apply filter settings to all function pages.

## Machine Group

Limits the display of data on all function pages by group ID.

## View

Change views by selecting a different view definition. The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type.

## Edit...

Click the **Edit...** button to display the **View Definitions** (page 28) page.

## Reset

Clears all filtering.

## Go to

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Show

Select the number of machines IDs displayed on each page.

## (Machine Count)

Shows the machine count, based on filter settings.

## View Definitions

Machine ID / Group ID Filter > Edit...

The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. You can create and name multiple views. View filtering is applied to *all* function pages by selecting a **View** from the drop-down list on the **machine ID / machine group filter** (*page 26*) panel and clicking the **Apply**  icon.

### Header Options

- **Save** - Save the selected view.
- **Save As** - Save the selected view view to a new name.
- **Delete** - Delete the selected view.
- **Select View** - Select a view.
- **Edit Title** - Edit the title of a view.
- **Share...** - You can **share** (*page 406*) a view with selected VSA users and user roles or make the view public for all VSA users and user roles.

### To Create or Edit a New View

1. Click the **Edit...** button to the right of the **View** drop-down list in the machine ID / group ID filter panel to open the **View Definitions** editor.
2. Click the **Save As** button and enter a name for a new view.
3. Enter the desired filter specifications.
4. Click the **Save** button.

### View by Machine ID

- **Set machine ID** - Checking this box overrides any value set for the **Machine ID** field on the Machine ID / Group ID filter panel with the value entered here. The Machine ID field on the Machine ID / Group ID filter panel is disabled to prevent inadvertent changes while displaying a view with **Set machine ID** selected.
- **Set group ID** - Checking this box overrides the **Group ID** filter on the Machine ID / Group ID filter panel with the value entered here. The Group ID field on the Machine ID / Group ID filter panel is disabled to prevent inadvertent changes while displaying a view with **Set group ID** selected.
- **Only show selected machine IDs** - Save a view first before selecting machines IDs using this option. Once the view is saved, a **<N> machines selected** link displays to the right of this option. Click this link to display a **Define Collection** window, which allows you to create a view using an arbitrary **collection** (*page 588*) of machine IDs.

### View by Network Status and Address

- **Show machines that have / have not / never been online in the last N periods** - Check to list those machines whose agents have checked into the KServer, or not, within the specified period of time. Use the **never** option to filter **machine ID template** (*page 592*) accounts, because these accounts never check in.
- **Show machines that are suspended / not suspended** - Check to list machines that are suspended or are not suspended.
- **Show machines that have/have not rebooted in the last N periods** - Check to list machines that have not rebooted in the specified number of periods.
- **Machines with Credential status** - Check to list machines with the selected **credential** (*page 588*) status.
- **Connection gateway filter** - Check to only list machines that have a connection gateway matching the specified filter. Include an asterisk (\*) wildcard with the text you enter to match multiple records. For example **66.221.11.\*** matches all connection gateway addresses from **66.221.11.1** through **66.221.11.254**.

- **IP address filter** - Check to only list machines that have an IP address matching the specified filter. Include an asterisk (\*) wildcard with the text you enter to match multiple records. For example 66.221.11.\* matches all IP addresses from 66.221.11.1 through 66.221.11.254.

### View by Operating System

- **OS Type** - Check to only list machines that match the selected operating system as reported by a Latest Audit.
- **OS Version** - Check to only list machines that match the OS version string as reported by a Latest Audit. Use this filter to identify machines by **service pack**.

### View Machines Based on Procedure History/Status

- **With agent procedure scheduled/not scheduled** - Check to only list machines that have the specified agent procedure either scheduled to run or not.

**Note:** Click the [select agent procedure](#) link to specify the agent procedure by name.

- **Last execution status success/failed** - Check to only list machines that have already executed the selected agent procedure. Select the appropriate radio button to list machines that successfully executed the agent procedure or failed to execute the agent procedure.
- **Agent procedure has/has not executed in the last N days** - Check to only list machines that have or have not executed the agent procedure in the specified period of time.

### View Machines by Application

- **Contains/Missing application** - Check to only list machines that have, or don't have, an application installed using the specified filter. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Version string is > < = N** - Check to further refine the application filter with a version number greater than, less than or equal to a specified value.

### View Machines by Patch Update

- **Show/Hide members of patch policy** - Checking this box works together with the machine ID and group ID filters to only list specific machines belonging (**Show**) or not belonging (**Hide**) to a specific **patch policy** (page 595).
- **Machines that have no patch scan results (unscanned)** - Check to only list machines that have not been scanned for missing patches.
- **Machines missing greater than or equal to N patches** - Check to only list machines *missing* a specified number of Microsoft patches.
- **Use Patch Policy** - Check to only list machines missing a specified number of *approved missing* Microsoft patches.
- **Patch scan schedule / not schedule** - Check to only list machines with either a patch scheduled or not scheduled.
- **Last execution status for patch scan success / failed** - Check to only list machines whose patch scan succeeded or failed.
- **Patch scan has / has not executed in the last <N> <periods>** - Check to only list machines whose patch scan has or has not executed within a specified time period.
- **Machines with Reboot Pending for patch installations** - Check to only list machines with a reboot pending for patch installations.
- **Machines with Patch Test Result** - Check to only list machines with the selected patch test result.
- **Machines with Patch Automatic Update configuration** - Check to only list machines with the selected **Automatic Update** (page 317) configuration.
- **Machines with Patch Reboot Action configuration** - Check to only list machines with the selected **Reboot Action** (page 337) configuration.
- **Machines with Patch File Source configuration** - Check to only list machines with the selected patch **File Source** (page 340) configuration.

## Agent

- **Machines missing a specific patch (identified by the patch's 6 digit KB Article ID)** - Check to only list machines missing a specific patch.

## View Machines by Agent Data

- **Advanced Agent Data Filter** - Check and click the **Define Filter...** button to further refine the view using the **Filter Aggregate Table** (page 30).

**Warning:** You must enter a space character to separate the operator from the data in a filter entry. For example, the filter entry `>= 500` includes a space character just after the equal sign.

## View Machines Monitoring Sets Assigned

- **Only show machines with monitorset assigned <Select a Monitorset>** - Select to list all machines assigned this monitor set.
- **Only show machines with monitorset assigned <Select a SNMPset>** - Select to list all machines assigned this SNMP set.

## Filter Aggregate Table

Machine ID / Group ID Filter > Edit... > Define Filter...

The **Filter Aggregate Table** lists over 75 agent and managed machine attributes that can be used to further refine a view definition using **advanced filtering** (page 30).

**Note:** **Collections** (page 588) provide an alternate method of selecting machine IDs for a view definition (page 28), regardless of whether they share any attributes.

## User Defined Attributes

You can add user defined attributes to the **Filter Aggregate Table** using the Audit > **System Information** (page 140) page, then create view definitions that select machine IDs based on these user defined attributes.

## Advanced Filtering

Advanced filtering lets you design complex searches to isolate data to just those values you want. Enter filter strings into the same edit fields you enter filter text.

**Warning:** You must enter a space character to separate the operator from the data in a filter entry. For example, the filter entry `>= 500` includes a space character just after the equal sign.

Advanced filtering supports the following operations:

### White Space

To search for white space in a string, enclose the string in double quotes.

For example: `"Microsoft Office*" OR "* Adobe *"`

### Nested operators

All equations are processed from left to right. Use parenthesis to override these defaults.

For example: `(("* adobe " OR *a*) AND *c*) OR NOT *d* AND < m`

## AND

Use the logical AND operator to search for data that must contain multiple values but can appear in different places in the string.

For example: `Microsoft* AND *Office*` returns all items that contain both Microsoft and Office in any order.

## OR

Use the logical OR operator to search for data that may contain multiple values but must contain at least one.

For example: `*Microsoft* OR *MS*` returns all items that contain either Microsoft and MS in any order.

## NOT

Search for a string not containing the match data.

For example: `NOT *Microsoft*` returns all non-Microsoft applications.

For example: `NOT *hotfix* AND NOT *update*` returns all items that do not contain either the strings `hotfix` or `update`.

## <, <= (Less than or less than or equal to)

Returns all data whose value is numerically less than, if a number. If this is alphabetic data then it returns all strings appearing earlier in the alphabet.

For example: `< G*` returns all applications starting with a letter less than "G".

For example: `< 3` returns all values numerically less than "3".

**Note:** Dates may also be tested for but must be in the following format: `YYYYMMDD HH:MM:SS` where `YYYY` is a four digit year, `MM` is a two digit month (01 to 12), `DD` is a two digit day (01 - 31), `HH` is a two digit hour (00 - 23), `MM` is a two digit minute (00 - 59), and `SS` is a two digit second (00 - 59). `HH:MM:SS` is optional. Date and time are separated with a space.

For example: `< 20040607 07:00:00` or `< "20040607 07:00:00"` returns all dates earlier than 7:00 on 7 June 2004. *Ensure a space exists after the < operator.*

## >, >= (Greater than or greater than or equal to)

Returns all data whose value is numerically greater than, if a number. If this is alphabetic data then it returns all strings appearing after it in the alphabet.

For example: `> G*` returns all applications starting with a letter greater than "G".

For example: `> 3` returns all values numerically greater than "3".

---

# Agent Status

## Agent > Agent Status

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Agent status alerts can be defined using [Monitoring > Alerts > Agent Status](#) (page 222).

The [Agent Status](#) page provides a summary view of a wide variety of agent data. You may choose all the data columns yourself to fully customize the view. Column and filter selections apply to each VSA user individually. Paging rows can be sorted by clicking column heading links.

- User defined columns of information can be added using the [Audit > System Information](#) (page 140) page. Once added, you can display them on this page and in the [Aggregate Table](#) report.

## Agent

- You can filter the display of machine IDs on any agent page using the [Show machines that have / have not / never been online in the last N periods](#) option in [View Definitions](#) (page 28).

## Select Columns...

Specify which columns of data to display and the order to display them in.

## Filter...

Click [Filter...](#) to display a [Filter Aggregate Table](#). Enter strings to filter the display of rows in the paging area. For example, to search for the machine ID that "jsmith" is logged on to, enter `jsmith` in the edit box next to [Current User](#). Include an asterisk (\*) wildcard with the text you enter to match multiple records.

## Reset Filter

Displays only if an advanced filter is set. Click [Reset Filter](#) to clear all filter strings.

## Column Definitions

Columns are described in the default order they display on this page.

- [Machine ID](#) - Machine ID label used throughout the system.
- [Current User](#) - Logon name of the machine user currently logged into the machine (if any).
- [Last Reboot Time](#) - Time of the last known reboot of the machine.
- [Last Checkin Time](#) - Most recent time when a machine checked into the KServer.
- [Group ID](#) - The group ID portion of the machine ID.
- [First Checkin Time](#) - Time when a machine first checked into the KServer.
- [Time Zone](#) - The time zone used by the machine.
- [Computer Name](#) - Computer name assigned to the machine.
- [Domain/Workgroup](#) - The workgroup or domain the computer belongs to.
- [Working Directory](#) - The directory on the managed machine the agent uses to store temporary files.
- [DNS Computer Name](#) - The fully qualified DNS computer name for the machine, which comprises the computer name plus the domain name. For example: `jsmithxp.acme.com`. Displays only the computer name if the machine is a member of a workgroup.
- [Agent GUID](#) - A unique identifier for a machine ID.group ID account and its corresponding agent.
- [Operating System](#) - Operation system type the machine is running.
- [OS Version](#) - Operation system version string.
- [IP Address](#) - IP address assigned to the machine, in version 4 format.
- [Subnet Mask](#) - Networking subnet assigned to the machine.
- [Default Gateway](#) - Default gateway assigned to the machine.
- [Connection Gateway](#) - IP address seen by the KServer when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
- [Country](#) - The country associated with the Connection Gateway.
- [IPv6 Address](#) - IP address assigned to the machine, in version 6 format.
- [MAC Address](#) - MAC address of the LAN card used to communicate with the KServer.
- [DNS Server 1, 2](#) - IP address of the DNS servers assigned to the machine.
- [DHCP Server](#) - The IP address of the DHCP server used by this machine.
- [Primary/Secondary WINS](#) - WINS settings.
- [CPU Type](#) - Processor make and model.
- [CPU Speed](#) - Clock speed of the processor.
- [CPU Count](#) - The number of CPUs.

- **RAM Size** - MBytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine.
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **Portal Access Logon** - Logon name given to a machine user for logging into the KServer.
- **Portal Access Remote Control** - Enabled if this machine user can log in and get remote control access *to their own machine from another machine*. Disabled if access is denied.
- **Portal Access Ticketing** - Enabled if this machine user can log in and enter trouble tickets. Disabled if access is denied.
- **Portal Access Chat** - Enabled if this machine user can *initiate* chat sessions with a VSA user. Disabled if access is denied.
- **Primary/Secondary KServer** - IP address / name the machine uses to communicate with the KServer.
- **Quick Checkin Period** - **Quick check in** (*page 588*) time setting in seconds.
- **Contact Name** - Machine user name entered in **Edit Profile** (*page 79*).
- **Contact Email** - Email address entered in Edit Profile.
- **Contact Phone** - Phone number entered in Edit Profile.
- **Contact Notes** - Notes entered in Edit Profile.
- **Manufacturer** - System manufacturer.
- **Product Name** - System product name.
- **System Version** - Product version number.
- **System Serial Number** - System serial number.
- **Chassis Serial Number** - Serial number on the enclosure.
- **Chassis Asset Tag** - Asset tag number on the enclosure.
- **External Bus Speed** - Motherboard bus speed.
- **Max Memory Size** - Max memory size the motherboard can hold.
- **Max Memory Slots** - Total number of memory module slots available.
- **Chassis Manufacturer** - Manufacturer of the enclosure.
- **Chassis Type** - Enclosure type.
- **Chassis Version** - Enclosure version number.
- **Motherboard Manufacturer** - Motherboard manufacturer.
- **Motherboard Product** - Motherboard product ID.
- **Motherboard Version** - Motherboard version number.
- **Motherboard Serial Num** - Motherboard serial number.
- **Processor Family** - Processor type installed.
- **Processor Manufacturer** - Processor manufacturer.
- **Processor Version** - Processor version ID.
- **CPU Max Speed** - Max processor speed supported.
- **CPU Current Speed** - Speed processor is currently running at.
- **vPro-Host Name** - The name of the vPro-enabled machine set by vPro configuration.
- **vPro-Computer Name** - The name of the vPro-enabled machine set by the operating system.
- **vPro-Model** - The model of the vPro-enabled machine.
- **vPro-Manufacturer** - The manufacturer of the vPro-enabled machine.
- **vPro-Version** - The version of the vPro-enabled machine.
- **vPro-Serial Number** - The serial number of the vPro-enabled machine.
- **vPro-Asset Number** - An asset management identifier assigned to the vPro-enabled machine.
- **vPro-Motherboard Manufacturer** - The manufacturer of the motherboard of the vPro-enabled machine.

## Agent

- **vPro-Motherboard Product Name** - The product name of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Version** - The version number of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Serial Number** - The serial number of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Asset Tag** - An asset management identifier assigned to the motherboard of the vPro-enabled machine.
- **vPro-Bios Vendor** - The vendor of the BIOS of the vPro-enabled machine.
- **vPro-Bios Version** - The version of the BIOS of the vPro-enabled machine.
- **vPro-Bios Release Date** - The BIOS release date of the vPro-enabled machine.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

---

## Agent Logs

### Agent > Agent Logs

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Agent Logs** page displays log data related to managed machines. There are corresponding **log reports** (page 149) for each type of log provided.

**Note:** The system automatically limits the number of log entries per log type per machine to 1000. Once the limit has been reached, log entries exceeding the limit are archived, if archiving is enabled, and deleted from the system. The archive option is set in **Log History** (page 35).

## Machine ID

Click the hyperlink of a machine ID to list all logs for that machine ID.

## Select Log

Select a log from the **Select Log** drop-down list. The types of logs available include:

- **Alarm Log** - Lists all alarms triggered for the selected machine.
- **Monitor Action Log** - The log of **alarm conditions** (page 585) that have occurred and the corresponding actions, if any, that have been taken in response to them.

**Note:** A counter value of -998 in the monitor logs indicates the monitor set is returning no data. Check that the **Performance Logs & Alerts service in Windows** is running. This is a pre-requisite for monitoring of performance counters.

- **Agent Log** - Displays a log of agent, system, and error messages.

- **Configuration Changes** - Displays VSA settings changes for the selected machine
- **Network Statistics** - Displays a log of send/receive data for network applications.

**Note:** This log requires the **Audit > Network Access** (page 87) driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is *disabled* by default.

- **Event Logs** - Displays event log data collected by Windows. Not available for Win9x. Only event logs that apply to the selected machine display in the event log drop-down list.
- **Agent Procedure Log** - Displays a log of successful/failed agent procedures.
- **Remote Control Log** - Displays a log of successful/failed remote control sessions.
- **Log Monitoring** - Displays **Log Monitoring** (page 591) entries.

### Events per Page

Select the number of rows displayed per page.

### Start Date / End Date / Refresh

Select a range of dates to filter log data, then click the **Refresh** button.

### Filter...

Applies to **Event Logs** only. Click **Filter...** to restrict the amount of data displayed. You can specify a different advanced filter for each event category and column of data displayed.

### Apply event log filter

Applies to **Event Logs** only. The event log filter includes options defined using the **Filter...** button. If **Applied event log filter** is checked, filtering is applied.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Log History

### Agent > Log History

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center*

The **Log History** page determines the number of days to store log data in the database on a per log basis for each machine ID. Log data is displayed using **Agent Logs** (page 34) or printed to a report using **Info Center > Reporting > Logs**. This page also determines whether agent log data is subsequently archived to text files located on a network directory. The directory is specified using **System > Configure** (page 412). Changes made using this page take effect at the next agent check-in and display **in red text** until then.

- **Log Settings** can also be maintained using the **Agent Settings** tab of **Live Connect** (page 380) > Agent Data or the **Machine Summary** (page 137) page.
- **System > Check-in Policy** (page 393) can restrict the number of days users can keep log entries, to avoid placing undue stress on servers running the KServer service.
- These settings default from the agent install package. Agent install packages are created using **Agent > Deploy Agent** (page 39).

### Estimating Database Sizing Requirements

The more data you log, the larger your database grows. Database sizing requirements can vary, depending on the number of agents deployed and the level of logging enabled. To estimate database sizing requirements for log data, create a dump of your database's `nteventlog` table. Determine how much data is being logged per day, then use that to predict the amount of extra space required to extend the log retention period.

### Log File Locations

Monitoring data log archives are stored in the `<KaseyaRoot>\UserProfiles\@dbBackup` directory. This is to improve performance on systems where the database is on a different server. All other agent log archives are stored in the directory specified by the System > **Configure** (page 412) > **Log file archive path** field.

### Set days to keep log entries, check to archive to file

Set the number of days to keep log data for each type of log. Check the checkbox for each log to archive log files past their cutoff date.

- **Agent Log** - The log of agent, system, and error messages.
- **Configuration Changes** - The log of configuration changes made by each user.
- **Network Statistics** - The log of incoming and outgoing packet count information and the application or process transmitting and/or receiving such packets. This information can be viewed in detail using Agent > **Agent Logs** (page 34) > Network Statistics.
- **Agent Procedure Log** - Displays a log of successful/failed agent procedures.
- **Remote Control Log** - Displays a log of remote control events.
- **Alarm Log** - The log of all alarms issued.
- **Monitor Action** - The log of alarm conditions that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **SYS log** - The log of all **System Check** (page 269) external systems.

### Set days to keep monitoring logs for all machines

The following monitoring log settings are applied system-wide.

- **Event Log** - The log of all events. The events collected are specified in more detail using Agent > **Event Log Settings** (page 37).
- **Monitor Log** - The log of data collected by monitoring sets.
- **SNMP Log** - The log of all data collected by SNMP sets.

### Set All Days

Click **Set All Days** to set all "day" fields to the same setting.

### Select All Archive / Unselect All Archive

Click the **Select All Archive** link to check all archive checkboxes on the page. Click the **Unselect All Archive** link to uncheck all archive checkboxes on the page.

### Update

Click **Update** to update selected machine IDs with agent log settings.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

---

# Event Log Settings

## Agent > Event Log Settings

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Event Log Settings](#) page specifies the [event log](#) (page 589) types and categories included in the [Log History](#) (page 35). *Event logs must be enabled for a machine ID before event log alerts can be configured for that machine ID using Monitoring > Alerts > Event Logs* (page 234). The list of event log types available on this page can be updated using Monitor > [Update Lists by Scan](#) (page 203).

To specify [Event Log Settings](#):

1. Click an event log type in the [Event Log Types](#) list box. Hold down the [Ctrl] key to click multiple event log types.
2. Click [Add >](#) to add event log types to the [Assigned Event Types](#) list box. Click [<< Remove](#) or [<< Remove all](#) to remove event log types from the [Assigned Event Types](#) list box.
3. Check one or more event categories: [Error](#), [Warning](#), [Information](#), [Success Audit](#), [Failure Audit](#), [Critical](#), [Verbose](#).
4. Select one or more machine IDs.
5. Click [Update](#) or [Replace](#) to apply these settings to selected machine IDs.

## Global Event Log Black Lists

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml`. The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

## Flood Detection

If 1000 events—not counting [black list events](#) (page 590)—are uploaded to the KServer by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your KServer. Alarm detection and processing operates regardless of whether collection is suspended.

## Agent

### Update

Adds event log types listed in the [Assigned Event Types](#) list box to the set of event log types already assigned to selected machine IDs.

### Replace

Replaces all event log types assigned to selected machine IDs with the event log types listed in the [Assigned Event Types](#) list.

### Clear All

Clears all event log types assigned to selected machine IDs.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Delete Icon

Click the delete icon  to delete this record.

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

### Assigned Categories

The event categories stored by the VSA for this machine ID and event log:

- [Error](#)
- [Warning](#)
- [Information](#)
- [Success Audit](#)
- [Failure Audit](#)
- [Critical](#) - Applies only to Vista, Windows 7 and Windows Server 2008
- [Verbose](#) - Applies only to Vista, Windows 7 and Windows Server 2008

---

# Deploy Agents

## Agent > Deploy Agents

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Deploy Agent** page creates and distributes an agent install package to *multiple* machines.

- Use Agent > **Create** (page 49) to create a machine ID account and agent install package in two separate steps and apply them to a *single* machine. You can also use **Create** to create **machine ID templates** (page 592) or re-install an agent for an *existing* machine ID.
- Use **Install Agents** (page 60) to install agents *on remote systems*.

**Note:** See System Requirements for a list of operating systems agents can be installed on.

**Note:** See the PDF quick start guide, Agent Configuration and Deployment. This and other resources are listed in the first topic of online help.

**Note:** An agent is automatically installed on the Kserver. You can click the check-in icon for this agent to initiate a **Live Connect** (page 380) session with the Kserver.

## Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** (page 592) and the **agent** (page 583). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

## Machine ID Templates

Machine ID template is a *machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc. **A corresponding install package can be created based on each machine ID template you define.**

- Create machine ID templates using Agent > **Create** (page 49).
- Import a machine ID template using Agent > **Import/Export** (page 71).
- Base an agent install package on a machine ID template using Agent > **Deploy Agents** (page 39).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** (page 70).
- Identify the total number of machine ID template accounts in your VSA using System > **Statistics** (page 423).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Macintosh and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

## Install Filenames

The full filename for a Windows agent install package is `KcsSetup.exe`. The full filename for a Macintosh agent install package is `KcsSetup.app`. `KcsSetup.app` is downloaded as a `KcsSetup.zip` which contains `KcsSetup.app` inside a folder titled `Agent`. Click the

## Agent

`KcsSetup.zip` file to expand it, click the `Agent` folder, then click the `KcsSetup.app` file to execute it.

### Using the Wizard

The **Deploy Agents** install package is created using a **Configure Automatic Account Creation** wizard. The wizard copies agent settings from an *existing* machine ID or machine ID template and generates an install package called `KcsSetup`. All settings and pending agent procedures from the machine ID you copy from—except the machine ID, group ID, and organization ID—are applied to every new machine ID created with the package.

### Including Credentials in Agent Install Packages

If necessary, an agent install package can be created that includes an administrator **credential** (page 588) to access a customer network. Credentials are only necessary if users are installing packages on machines and *do not have administrator access* to their network. The administrator credential is encrypted, never available in clear text form, and bound to the install package.

### Editing Existing Install Packages

Typically an existing **Deploy Agents** install package is edited just before re-distribution. The most common changes made to an install package are:

- Pre-selecting an organization ID, group ID or sub-group ID.
- Assigning a credential, if necessary.

Once edited, the install package can be re-created and distributed to the specific customer and location it is intended for.

### Distribution Methods

Once created, you can use the following methods to distribute an agent install package:

- **Logon**
  - **Windows** - Set up an **NT logon** procedure to run the install package every time a user logs into the network. See system requirements.
  - **Macintosh** - Set up an **Mac OS X Login Hook Procedure** to run the install package every time a user logs into the network. See Apple KB Article **HT2420** (<http://support.apple.com/kb/HT2420>).

#### Procedure

1. Create the deployment package using the Agent > **Deploy Agents** wizard.
  - ✓ The `KcsSetup` installer skips installation if it detects an agent is already on a machine if the `/e` switch is present in the installer package.
  - ✓ You will probably want to select the silent install option.
  - ✓ It may be necessary to bind a administrator credential if users running the logon procedure don't have user rights.
2. Download the appropriate `KcsSetup` installer package using the `dl.asp` page and copy it to a network share which users can execute programs from.
3. Add `KcsSetup` with its network path to the logon procedure.
  - **Email** - Email `KcsSetup` to all users on the network. Download the appropriate install package from the **Deploy Agents** page, then attach it to an email on your local machine. You can also copy and paste the link of the default install package into an email message. Include instructions for launching the package, as described in the **Manual** bullet below.
  - **LAN Watch** - Users can discover newly added machines during a **LAN Watch** (page 56) and subsequently install agents *remotely* using the Agent > **Install Agents** (page 60) page.
  - **Active Directory** - Run LAN Watch on an Active Directory machine. From then on, Windows agents can be installed automatically on Windows machines as soon as users logon using Active

Directory. See [View AD Computers](#) (page 65) and [View AD Users](#) (page 66). Macintosh and Linux are not supported.

- **Manual** - You can instruct users to download an install package agent from the `http://<VSA_Address>/dl.asp` website to their target machines. If more than one install package is displayed on the website, instruct users which package should be selected. Users can execute the `KcsSetup` installer using any of the following methods:

- **Windows**

- ✓ Double click `KcsSetup` to launch it.
- ✓ Open a **command line window** and type `KcsSetup` followed by any desired **command line switches** (page 44).
- ✓ Select **Run...** from the **Windows Start** menu and type `KcsSetup` followed by any desired command line switches.

- **Macintosh and Linux**

- ✓ Double click `KcsSetup` to launch it.
- ✓ Open a **terminal process**, navigate to where `KcsSetup` is located and launch `KcsSetup`.

**Note:** For Macintosh, **command line switches** (page 44) can only be used when creating the agent install package.

**Note:** For Linux, see [Installing Linux Agents](#) (page 47) for more detailed instructions.

## Default User Install Packages

Each user can specify their own default install package by selecting the **Set Default** radio button to the left of the package name. Users can download their own default agent immediately by selecting the [Click to download default Agent](#) link on the [Deploy Agents](#) page.

## Unique ID Number

You can tell users which install package to download by referencing the install package's *unique ID number*. Example: `http://<VSA_Address>/dl.asp?id=123`. The default install package is displayed with its unique ID number in the header of the [Deploy Agents](#) page.

## Assigning New Machine IDs to Machine Group by IP Address

Maintaining multiple agent install packages in Agent > [Deploy Agents](#) (page 39), one for each organization, can be time consuming. Instead some server providers use a single agent package for the unnamed organization and perform all installs using this package. System > [Naming Policy](#) (page 395) can reassign new agents to the correct organization.group ID automatically—the first time the agents check in—based on each managed machine's IP or connection gateway. Agent > [Copy Settings](#) (page 70) may be used afterwards, to manually copy specific kinds of agent settings by [machine ID template](#) (page 592) to the type of machine revealed by the initial audit.

## Automatic Account Creation

You must have *automatic account creation enabled* using System > [Check-in Policy](#) (page 393) to automatically create a machine ID account when a [Deploy Agents](#) package is installed.

## Operating System Selection

Agent packages can be created to install agents on machines running either Windows, Macintosh, or Linux operating systems, or to automatically choose the type of operating system of the downloading computer.

## Create Package

Click [Create Package](#) to start a [Configure Automatic Account Creation](#) wizard where you can specify all

configuration parameters for the install package. The wizard is a 7 step process.

1. Define rules for naming the machine ID.
  - Prompt the user to enter a machine ID.
  - Use the computer name as the machine ID.
  - Set the user name of the currently logged on user as the machine ID.
  - Specify a fixed machine ID for this install package.
2. Define rules for naming the group ID.
  - **Existing Group** - Select an existing group ID from a drop-down list.
  - **Domain Name** - Uses the user's domain name.
  - **New Group** - Specify a new group ID. This option only displays for **master role users** (page 600).
  - **Prompt User** - Asks user to enter a group ID. This option only displays for **master role users** (page 600).
3. Specify agent install package **command line switches** (page 44) including the ability to install **silently without any task bars or dialog boxes** (page 597).
4. Specify the machine ID to copy settings and pending agent procedures from. All copied settings and pending agent procedures—except the organization ID, machine ID, and group ID—are applied to every new machine ID created with the package.

**Note:** The statement `Copy settings from unknown.root.unnamed if nothing selected is based on the machine ID or template selected by the Default Install package. See Editing the Default Install Package below.`

5. Select the operating system you are creating the install package for: Automatically choose OS of downloading computer: Windows, Macintosh, or Linux.
6. Optionally bind a user logon credential to the install package. Fill in the **Administrator Credential** form to securely bind user rights to the install package.
  - Users without administrator rights can install the package successfully without having to enter an administrator credential.
  - If the administrator credential is left blank and the user does not have administrator rights to install software, the install package prompts the user to enter an administrator credential during the install. **If the package is also silent KcsSetup will fail without any dialog messages explaining this.**
7. Name the install package for easy reference later. This name displays on the **Deploy Agents** page and the `dl.asp` download page.

**Note:** Credentials are only necessary if users are installing packages on machines and do not have administrator access to their network.

### Install Issues and Failures

See **Install Issues and Failures** (page 45) if an agent fails to install.

### Editing the Default Install Package

The `Default Install` package sets the default values displayed when you create a new package. Normally the `Default Install` package cannot be modified. The **Save** button is disabled. To enable the **Save** button for the `Default Install` package, do the following as a *master role user*:

1. Click the **Share** button next to the `Default Install` package in Agent > **Deploy Agents**.
2. Click Take Ownership.
3. Check **Allow other users to modify**.
4. Click **Save**.
5. Click the edit icon  next to the `Default Install` package.

The **Save** button will be enabled when you edit the `Default Install` package.

**Note:** If you delete the `Default Install` package, it is re-created immediately.

### Click to download default Agent

Click this link to download the current VSA user's default package directly from this page.

### Users can download agents from

Paste this hyperlink into an email message. The *unique ID number* ensures that when the link is clicked in the email message, the default install package is selected and downloaded. Set a different install package as the default to display the link for that install package.

### Manage packages from all administrator

Check to display all packages created by all VSA users. Once a hidden package is displayed, you can use the package, make the package public or take ownership. This option only displays for **master role users** (page 600).

### Set Default

Specify your own default install package by selecting the radio button to the left of the package name in the **Set Default** column.

### Delete Icon

Click the delete icon  to remove a package from the paging area. If you created the package, then this also deletes the package from the system and removes it for all VSA users.

### Edit Icon

Click the edit icon  next to a package to change parameters for that package using the **Configure Automatic Account Creation** wizard.

### Package Name

Lists the name of the package.

### Public Package

Public package rows display with a brown background. Private package rows display with a gray background.

### Share

Click **Share** to **share** (page 406) a private package with other users, user roles or to make the package public.

### List on dl.asp

Click the **dl.asp** link in the column header to display the web page machine users see when they install an agent on their machine. Check a box in this column to include its package in the list of available download packages on the **dl.asp** page.

### Description

Displays the description of the package.

## Agent Install Command Line Switches

Agent install command line switches for `KcsSetup` are case insensitive and order independent. Separate switches with an empty space. For example: `KcsSetup /e /g=root.unnamed /c`

**Note:** For Macintosh agents, command line switches can only be used when creating the agent install package.

`/b` - Reboot the system after installation completes. Agent installation requires a reboot in order to load its drivers. Use this switch on packages given to users that do not have rights to shut down the computer.

`/c` - Use the computer name as the machine ID for the new account. If the computer name cannot be determined programmatically, the machine user is prompted to enter a machine ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/d` - Use the current domain name as the group ID for the new account. If the domain name cannot be determined programmatically, the machine user is prompted to enter the group ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/e` - Exit immediately if the installer detects that an agent is already installed. Use `/e` at the end of logon procedures. `/k` or `/r` overrides `/e`.

`/f "Publisher"` - Specifies the full name of the service provider or tenant. Windows only.

`/g=xxx` - Specifies the group ID to use for the new account. `xxx` must be an alpha-numeric string and can not contain spaces or punctuation marks.

`/h` - Display the help dialog box listing all the command line switches, unless the `/s` switch is set, in which case the application exits.

`/i` - Ignore non-critical errors such as incorrect or indeterminate versions of WinSock2, or indeterminate versions of the OS, and force the installation to proceed.

`/j` - Does not install an agent shortcut to the **Start > All Programs** menu. Windows only.

`/k` - Displays a dialog box asking the user if it is OK to re-install when the agent is already detected on the machine. Without this switch, the installer exits if an agent is already present.

`/m=xxx` - Specifies the machine ID to use for the new account. `xxx` must be an alpha-numeric string and can not contain spaces or any punctuation marks except period(.).

`/n = partitionId` - Specifies the tenant the installed agent/machine ID account is a member of.

`/o "Company Title"` - Specifies the company title of the service provider or tenant. Windows only.

`/p "install_path"` - Overrides the default installation path by specifying the full directory path, including drive letter, in which to install the agent. By default, the agent installation creates a directory named `Program Files\Kaseya\Agent` off the root of the drive on which Windows is installed.

`/r` - Executes the installation program and re-installs the agent even if an agent is already on the machine.

`/s` - Runs in silent mode. Suppresses all dialog boxes.

`/t "Title"` - Specifies the title of any dialog windows shown to the machine user during installation. The default title is: "Kaseya Agent".

`/u` - Uses the current machine user name as the machine ID for the new account. If the machine user name cannot be determined programmatically, the user is prompted to enter a machine ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/w` - Overwrites the existing configuration file with a configuration file included in the agent installation. Use with the `/r` switch to re-install an agent with new server settings. Intended for an existing agent that is attempting to connect to a server that no longer exists.

`/x` - Disables remote control after successfully installing the agent. This option is ignored when updating or re-installing. Remote control of this machine can only occur after the user selects **Enable Remote Control** by right clicking the K icon  on the system tray.

`/z "Message"` - Specifies the message shown to the user when installation completes. The exception is silent mode, `/s`, in which case the installation completes and the status message is written to the installation log. The default message is: "The Agent has been installed successfully on your computer."

`/?` = Display the help dialog box listing all the command line switches, unless the `/s` switch is set, in which case the application exits. Windows only.

## Install Issues and Failures

The following issues and failures can occur when installing agents:

- **Invalid Credential** - The **credential** (*page 588*) bound to the package must have administrator rights on the local machine. The agent installs as a system service requiring full administrator privileges to install successfully. The administrator name may be a domain user of the form `domain\administrator` or `administrator@domain`. On Vista, 7, and 2008 machines, ensure User Account Control (UAC) is disabled for the administrator rights credential being used.
- **Domain Specified for a Machine Not in the Domain** - If, in step 2 of package creation in **Deploy Agent**, the **Domain Name** option is selected and the computer is not part of a domain, an installation package will peg the CPU at 100% during install, but eventually install.
- **Blocked by Anti-Virus Program** - Some anti-virus programs may classify the agent installation as a security threat and block its execution.
- **Blocked by Security Policy** - Local or domain security policies may prevent access to the installation directory, typically by default the `Program Files` directory.
- **Insufficient Licenses** - The agent may be prevented from checking in the first time and creating an account if there are insufficient VSA licenses available. When this happens a gray K icon appears in the system tray just after the agent is installed on the machine and never turns blue. A tooltip displays when the cursor is placed over the gray agent icon and reports "'Machine ID.Group ID' not recognized by the KServer".

### Macintosh

- Macintosh agents cannot be deployed silently without a valid username and password.

### Using Active Directory

These types of failures apply when an agent is installed using **View AD Computers** (*page 65*) or **View AD Users** (*page 65*):

- **Port Blocked** - Active Directory agent deployment will fail if the KServer assigned port is blocked by a firewall.
- **Authentication Requirement for AD Imported Users** - The domain controller that performs the authentication must have **Authenticated users** set as a member of **Local Security policy - Access this computer from the network**.

=====

## Installing Multiple Agents

Multiple agents can be installed on the same managed machine, each checking in to different

## Agent

### KServers.

- A v6 agent can co-exist with v5.1 or older agents.
- A v6 agent can co-exist with other v6 agents.
- *Run the v6 agent installer from a different KServer* and you will get an additional agent.
- Any managed machine with a domain controller login procedure that runs the agent installer automatically *must* update the v5.1 or older `KcsSetup` file with the v6 agent. The v5.1 or older installer does not know about the newer v6 agent and will re-install even if the v6 agent is present.
- Installing multiple Macintosh agents is not supported.

## Driver Usage

If multiple agents are installed on a machine, only one agent at a time controls the drivers required to use [File Access](#) (page 85), [Network Access](#) (page 87), [Application Blocker](#) (page 89). These functions can only be performed by the agent controlling these drivers.

- Originally the first agent installed controls the drivers.
- If the first agent controlling the drivers is uninstalled, then these drivers are uninstalled as well and these three functions cannot be performed by any agent.
- These drivers are re-installed by either of the following events:
  - Any of the existing agents on the machine are updated. The updated agent takes control of the drivers and can perform these three functions.
  - A new agent is installed. The newly installed agent takes control of these drivers and can perform these three functions.
- To determine which agent has control of the drivers, see *Registry* below.

## Identifying Agents on Managed Machines

When a Kaseya agent is installed, a *unique identifier* is created for the agent comprising the KServer's 6 character customer ID and a randomly generated 14 digit number. This unique agent identifier, called the agent GUID, is used to create separate sub-folders to store agent program files, and as a sub-key for agent registry values.

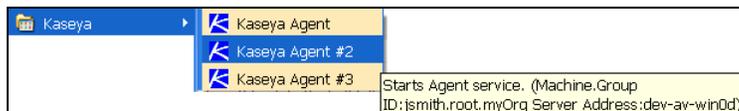
In the examples below, agents display specific information for the following placeholders:

- `<GUID>` - The agent's GUID.
- `<company>` - The agent's install directory.
- `<serveraddress>` - The KServer address the agent checks into.
- `<machineID.groupID.orgID>` - The machine ID, group ID, and organization ID of the agent on the KServer.
- `<shortcutname>` - The name of the shortcut. Example: `Kaseya Agent #2`.

## Shortcuts

When you move the mouse cursor over a Kaseya Agent shortcut—for example, a shortcut on the Windows Start Menu—a tool tip displays as:

- Start Agent service. (machine.GroupID:<machineID.groupID.orgID> Address:<serveraddress>)
- If you right click a shortcut, you'll also see this text in the comment field of the shortcut property page.



## About Agent

Right click the K icon  in the system tray of a managed machine and select the [About Agent](#) option to

display the following information:

- Agent Version
- Server Address - <serveraddress>
- Product ID - <GUID>
- Program Title - <shortcutname>

### Add/Remove

Agents display as follows:

- Kaseya Agent (<machineID.groupID.orgID> - <serveraddress>)
- Kaseya Agent #2 (<machineID.groupID.orgID> - <serveraddress>)
- Kaseya Agent #3 (<machineID.groupID.orgID> - <serveraddress>)

### Services

The description field of the service displays the same text shown above in the agent shortcut.

### Registry

Agent registry settings displays as follows:

```
HKLM\Software\Kaseya\Agent
  DriverControl - The agent that controls driver usage.
  KES_Owned_By - The agent that manages the KES client.
```

```
HKLM\Software\Kaseya\Agent\<GUID>
  Title - <shortcutname>
  Path - C:\Program Files\<company>\<GUID>
  ServAddr - <serveraddress>
  machineID - <machineID.groupID.orgID>
  DriverControl - The agent that controls driver usage.
  KES_Owned - The agent that manages the KES client.
```

### Agent Installation Folder

```
%ProgramFiles%\<company>\<GUID>
```

## Installing Linux Agents

**Note:** See System Requirements for supported Linux operating systems and browsers.

### Installing Linux Agents Manually

1. From a Linux machine open a Firefox or Chrome browser in a Gnome session and log into the VSA.
2. Display the Agent > Install Agents > **Deploy Agents** (page 39) page.
3. Click the **Click to download default Agent** hyperlink to begin downloading the the default agent install package. A Linux agent install package will download.

**Note:** Alternately, you can create your own Linux package by pressing **Create Package** and stepping through the wizard.

4. Once the download is complete, locate the `KcsSetup.sh` file in the download directory of the Linux machine.

**Note:** If you have downloaded `KcsSetup.exe` or `KcsSetup.zip`, you have downloaded the wrong install file because the selected install package is dedicated to Windows or Macintosh installs.

5. Issue the following commands as root:

```
# chmod +x KcsSetup.sh
# ./KcsSetup.sh
```

The agent installs and starts. Log into your VSA and view the status of the agent.

For further information see the install log file, located at:

```
/tmp/KASetup_<pid>.log
```

where <pid> is the process id of the `./KcsSetup.sh` execution.

6. After the Linux agent is installed, log in and log out to see the Kaseya agent icon in a Gnome panel.

**Note:** The agent icon program, `KaUsrTsk`, is not currently supported on SuSE Enterprise Linux 10.

### Installing Linux Agents Using LAN Watch and Install Agents

1. Schedule a [LAN Watch](#) (page 56) scan using an existing Linux agent as the discovery machine.
2. Install a Linux agent on a discovered Linux machine, using the [Install Agents](#) (page 60) page.
  - Enter `root` in the **Admin Logon** field.
  - Enter the password for the `root` user of the targeted Linux machines in the **Password** field.
  - Select an agent install package in the **Select an Agent Package to install** field.
  - Check the checkboxes next to one or more targeted Linux machines, or enter the IP address or name of a targeted Linux machine in the **undiscovered machine** field.
  - Click the **Submit** button.

**Note:** The [Install Agents](#) page does not currently distinguish between Linux and other systems. It is the installer's responsibility to select only Linux systems.

### Uninstalling a Linux Agent Manually

A `<install-dir>/bin/KcsUninstaller` always gets installed with the agent and will remove the agent. Agents are typically installed to the `/opt` directory. Run the command `./KcsUninstaller -D -v` to uninstall the agent.

## Supported Linux Functions

Linux agents support the following functions:

- Agent procedures
- Latest audits, baselines audits and system audits
- Remote control and FTP with VNC
- Reset Password
- LAN Watch and Install Agents - See [Installing Linux Agents](#) (page 47).
- Site Customization - The **Agent Icons** tab now includes a set of icons for Linux agents you can customize.
- Only non-plug-in specific items are accessible via a Linux-based Browser or when browsing to Linux agent machine. This is the following:
- Live Connect - Only non-plug-in specific items are accessible via a Linux-based browser or when browsing to a Linux agent machine. Supported menu options include:
  - Home
  - Agent Data
  - Audit Information

- Ticketing (or Service Desk Ticketing)
- Chat
- Video Chat

See System Requirements.

## Supported Macintosh Functions

Macintosh agents support the following functions:

- Audits - selected hardware and software attributes
- Agent procedures
- Remote Control
- FTP
- Reset Password
- Task Manager
- Live Connect including Desktop Access.
  - On Mac Leopard (Intel), you can use Desktop Access in Live Connect to remote control a Windows system using Firefox or Safari.
  - On Windows using any of our supported browsers you can use Desktop Access to remote control a Mac Leopard (Intel) system.
  - Does not include a thumbnail preview image of the desktop in Live Connect.
- LAN Watch / Install Agents
- Supported monitoring:
  - SNMP monitoring
  - Process monitoring in monitor sets

See System Requirements.

---

## Create

### Agent > Create

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Create** page creates a machine ID account and agent install package for a *single* machine. You create the machine ID account first, then create an install package for this single machine. Typically the **Create** page applies to:

- **Machine ID templates** - In this case, no install package need be created, since **machine ID templates** (page 592) are not intended for installation to a machine.
- **Secured environments** - Secured environments may require each machine be setup manually. For example, you might be required to name a new machine ID account manually and/or create an agent install package with a unique credential for a single machine. A user must be logged into a target machine locally to install the package.

**Note:** Use **Agent > Deploy Agents** (page 39) to create and distribute agent install packages to *multiple* machines. The **Deploy Agents** install package *automatically creates a machine ID account* when it is installed provided automatic account creation is enabled using **System > Check-in Policy** (page 393).

**Note:** Use **Install Agent** (page 60) to install agents *on remote systems*.

## Re-Installing Agents

Because the **Create** install packages does *not automatically create a new machine ID account*, you can use the **Create** page to *re-install* agents on managed machines for *existing* accounts.

## Agent

### Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** (page 592) and the **agent** (page 583). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

### Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a **machine ID template** (page 592). Machine ID template accounts are not counted as "used" until you install the agent.

### Including Credentials in Agent Install Packages

If necessary, an agent install package can be created that includes an administrator **credential** (page 588) to access a customer network. Credentials are only necessary if users are installing packages on machines and *do not have administrator access* to their network. The administrator credential is encrypted, never available in clear text form, and bound to the install package.

### Operating System Selection

Agent packages can be created to install agents on machines running either Windows, Macintosh, or Linux operating systems, or to automatically choose the type of operating system of the downloading computer.

### Machine ID Templates

Machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc. **A corresponding install package can be created based on each machine ID template you define.**

- Create machine ID templates using Agent > **Create** (page 49).
- Import a machine ID template using Agent > **Import/Export** (page 71).
- Base an agent install package on a machine ID template using Agent > **Deploy Agents** (page 39).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** (page 70).
- Identify the total number of machine ID template accounts in your VSA using System > **Statistics** (page 423).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Macintosh and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

### Predefined Alerts

If you create a machine ID account using Agent > **Create** and *do not copy settings from any other*

*machine*, then several typical alerts are created for the machine ID account by default.

### Copy new account settings from

Click a radio button next to any machine ID listed in the paging area. Agent settings are copied from this machine ID.

**Note:** If you don't include a machine ID to copy from and click **Create**, a new, usable machine ID account is created using KServer defaults.

### New Machine ID

Enter a unique name for the new machine ID you are creating.

### Group ID

Select an existing group ID for the new machine ID you are creating. The default is `root.unnamed`. Group IDs are created by a VSA user using System > Orgs / Groups / Depts > **Manage** (page 408).

### Create

Click **Create** to create the new machine ID for the selected group ID.

### Set/Clear New accounts created in group ID <Group ID> copy settings from <Machine ID>

For each group ID you can specify a different default machine ID to copy settings from.

1. Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area.
2. Select a group ID from the group ID drop-down list.
3. Click the **Set** to ensure that new machine IDs you create for the selected group ID will copy settings from the selected default machine ID.
4. Click the **Clear** link to remove this assignment.

### Set/Clear Accounts created in unassigned group IDs copy settings from <Machine ID>

This option specifies the default machine ID to copy settings from if no default machine ID is set for a group ID. This option only displays for **master role users** (page 600).

1. Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area. Initially this value is set to *unassigned*.
2. Click the **Set** to ensure that new machine IDs created without a group default machine ID copy settings from the master role user's default machine ID. Initially this value is set to *unassigned*.
3. Click the **Clear** link to remove this assignment.

### Entering Contact Information

When you enter contact information on this page for a new machine ID account, then create the new machine ID account by clicking the **Create** button, these same contact information fields populate the Agent > **Edit Profile** (page 79) page. Contact information includes:

- **Contact Email** - Enter the email address of the individual using the managed machine.
- **Auto** - Check **Auto** to automatically populate the **Contact Email** field with an email address that uses the following format: `machineid@groupid.com`. This feature assumes you are creating machine IDs and group IDs that conform to user email addresses.
- **Contact Name** - Enter the name of the individual using the managed machine.
- **Contact Phone** - Enter the phone number of the individual using the managed machine.

## Agent

- **Admin Email** - Enter the email address of the individual responsible for providing IT support for the managed machine.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Copy Settings

Click a radio button next to any machine ID listed in the paging area. Machine ID settings are copied from this machine ID.

## Download / Email Agent Installation

Click a machine ID link to create and distribute an install package for an existing machine ID account using the **Download Agent** wizard.

**Note:** An install package created using this page is for a specific machine ID account. Use **Deploy Agent** (page 39) to create install packages for *multiple* machines.

1. Select the operating system you are creating the install package for: Windows, Macintosh, or Linux.
2. Optionally bind a user logon credential to the install package. Fill in the Administrator Credential form to securely bind user rights to the install package.
  - Users without user rights can install the package successfully without having to enter an administrator credential.
  - If the administrator credential is left blank and the user does not have user rights to install software, the install package prompts the user to enter a administrator credential during the install.
3. Select the method of distribution.
  - **Download** - Download the install package immediately to the machine you are currently using. The install package is always called `KcsSetup`.
  - **Email** - Email a text message that contains a link to download the install package.

## Type

The type of operating system used by the managed machine:

- Windows
- Macintosh
- Linux

## First Checkin

Lists the time that each agent checked into the KServer for the first time.

---

# Delete

## Agent > Delete

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Delete** page deletes three different combinations of *machine ID accounts* and *agents*.

## Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** (page 592) and the **agent** (page 583). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

## Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a **machine ID template** (page 592). Machine ID template accounts are not counted as "used" until you install the agent.

## Procedure

1. Select one or more machine IDs in the paging area.
2. Click one of the following radio buttons:
  - **Uninstall agent first at next check-in** - Uninstall the agent from the machine **and** remove the machine ID account from the KServer. The account is not deleted until the next time the agent successfully checks in.
  - **Delete account now without uninstalling the agent** - Leave the agent installed **and** remove the machine ID account from the KServer.
  - **Uninstall the agent and keep the account** - Uninstall the agent from the machine **without** removing the machine ID account from the KServer.
3. Click the **Delete Accounts** button.

**Note:** Uninstalling an agent does not remove the installed Remote Control package, KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > **Uninstall RC** (page 366) to uninstall remote control on the managed machine. Uninstall all add-on module clients as well.

## Select old accounts that have not checked in since <date>.

Click the **Select old** hyperlink to check all machine IDs in the paging area that have not checked in since the specified date. This is an easy way to identify and remove obsolete machine IDs.

## Clean Database

Removing a machine account using this **Delete** page marks the machine account for deletion. Actual deletion usually occurs during off hours to reserve resources during working hours. There are some cases where it is useful to purge machine accounts immediately. For example, your KServer may

## Agent

exceed the agent license count. Click [Clean Database](#) to immediately purge machine accounts that are already marked for deletion.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Last Check-In

Displays the time the machine's agent last checked in to the KServer. Agents that have not checked-in recently display this information **in red text**.

---

## Rename

### Agent > Rename

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Rename](#) page renames any existing machine ID account. You can change the machine ID and/or re-assign it to a different group ID.

Agents are identified by a unique GUID number. Renaming the agent only changes the name the agent displays, both on the KServer and in the [Set Account...](#) option on the agent menu of the managed machine.

**Note:** See [Agent > Change Group](#) (page 56) to assign multiple machines to a different group ID.

### Procedure

1. Select a machine ID in the paging area.
2. Click one of the following radio buttons:
  - [Rename account](#) - Select this option to rename a selected machine ID account.
  - [Merge offline account <Offline Machine ID> into <Select Machine ID> Delete <Offline Machine ID> after merge](#) - Use merge to combine log data from two different accounts into the same machine. This could be necessary if an agent was uninstalled and then re-installed with a different account name. Merge combines the accounts as follows:

- ✓ Log data from both accounts are combined.
- ✓ **Baseline Audit** (page 587) data from the old offline account replaces any baseline data in the selected account.
- ✓ Alert settings from the selected account are kept.
- ✓ Pending agent procedures from the selected account are kept. Pending agent procedures from the old offline account are discarded.
- ✓ The old account is deleted after the merge.

**Note:** Since the machine can only be active on a single account, only offline accounts are provided in the drop-down list to merge with.

3. Optionally enter in a **New Name** for the machine ID account.
4. Optionally select a different **Group ID** for the machine ID account.
5. Click the **Rename** button.

### Rename

Click **Rename** to change the name of a selected machine ID account, using the options previously selected.

### New Name

Enter the **New Name** for the selected machine ID.

### Group ID

Select the **Group ID** to assign to the selected machine ID account. The default leaves the group ID unchanged.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404). Click the radio button to the left of the machine account you wish to rename.

### New Name at Next Check-in

Lists the new name the account will be renamed to the next time that agent checks in. Only pending renames are displayed here.

---

## Change Group

### Agent > Change Group

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Change Group** page assigns multiple machines IDs to a different group ID. Machines currently offline are assigned the next time they check in.

### Moving a Machine ID to a Different Group

- Select one or more machine IDs in the paging area.
- Select a group ID from the **Select new group ID** drop-down menu.
- Click the **Move** button.

### Move

Assigns selected machine IDs to the selected group ID.

### Select new group ID

Specify the new group ID to assign to each selected machine ID.

**Note:** Create a new machine group ID or sub group ID using [System > User Security > Scopes \(page 404\)](#).

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window (page 583)**.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs (page 592)** displayed is based on the **Machine ID / Group ID filter (page 26)** and the machine groups the user is authorized to see using [System > User Security > Scopes \(page 404\)](#).

---

## LAN Watch

### Monitor > LAN Watch

### Agent > LAN Watch

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

LAN Watch uses an existing VSA [agent](#) (page 583) on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without agents or [SNMP devices](#) (page 597). Optionally, the VSA can send an [alert](#) (page 585) when a LAN Watch discovers any new device. LAN Watch effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

### Using Multiple Machines on the Same LAN

Typically, you do not have to run a LAN Watch on more than one machine in a scan range. Some reasons to do a LAN Watch on multiple machines within the same scan range include:

- There are multiple SNMP Communities within the same scan range and therefore there are multiple machines with different SNMP Community Read values.
- There are multiple vPro-enabled credentials required.
- There are different alert configurations required.
- The user wishes to have redundant SNMP monitoring.

### Using the Same Operating System for Discovery and Agent Installs

Windows, Macintosh, and Linux agents can discover Windows, Macintosh, and Linux machines on the same LAN using [LAN Watch](#) (page 56). Agent > [Install Agents](#) (page 60) can only install agents on:

- Windows machines if the LAN Watch discovery machine was a Windows machine.
- Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.
- Linux machines if the LAN Watch discovery machine was a Linux machine.

**Note:** Macintosh agent install packages require a credential when using Agent > Install Agent, or when installing agents using the /s "silent install" switch.

**Note:** For Linux machines, the `root` username alone—without a hostname or domain—must be used.

### LAN Watch and SNMP

The LAN Watch discovery machine issues the SNMP requests to the SNMP devices it discovers on the same LAN. So you must run LAN Watch *first* to have access to SNMP-enabled devices using the VSA.

To include SNMP devices in the discovery scan performed by LAN Watch:

1. Select a machine ID on the same LAN as the SNMP devices you want to discover.
2. Specify the IP range to scan using the [Scan IP Range](#) fields. The fields default to the first 1024 IP addresses your selected machine ID belongs to.
3. Check the [Enable SNMP](#) checkbox.
4. Enter a `community` name in the [Read Community Name](#) and [Confirm](#) fields.  
A community name is a credential for gaining access to an SNMP-enabled device. The default "read" community name is typically `public`, in all lower case, but each device may be configured differently. You may have to identify or reset the community name on the device directly if you're not sure what community name to use.
5. Click the [Schedule](#) button, select scheduling parameters, then click the [Submit](#) button. The [Schedule](#) dialog closes.
  - The [Last Scan Started](#) displays the time the LAN Watch started scanning, once it has begun.
  - The [SNMP Active](#) column confirms that SNMP-enabled devices are being scanned as part of the LAN Watch.
6. Review discovered SNMP-enabled devices using the Monitor > Assign SNMP page.

### Schedule

Click [Schedule](#) to display the [Scheduler](#) window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly,

## Agent

Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

## Cancel

Click **Cancel** to stop the scheduled scan. Cancel also deletes all records of the devices identified on a LAN from the VSA. If you re-schedule LAN Watch after clicking Cancel, each device on the LAN is re-identified as though for the first time.

## Scan IP Range

Set the minimum and maximum IP addresses to scan here. Selecting a machine ID to scan, by checking the box next to that machine's name, automatically fills in the minimum and maximum IP range based on that machine's IP address and subnet mask.

**Note:** LAN Watch does not scan more than 2048 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch limits it to 2048 addresses. LAN Watch only detects addresses on the local subnet to the machine you run LAN Watch from. For example, with a subnet mask of 255.255.255.0, there can be no more than 253 other devices on the local subnet.

## Enable SNMP

If checked, scan for **SNMP devices** (page 597) within the specified **Scan IP Range**.

## Read Community Name / Confirm

LAN Watch can only identify SNMP devices that share the same **SNMP Community** (page 597) *Read* value as the managed machine performing the LAN Watch. Enter the value in the **Read Community Name** and **Confirm** text boxes.

**Note:** Community names are *case sensitive*. Typically the default read community name value is `public`, but may be reset by an administrator to `Public`, `PUBLIC`, etc.

## Enable vPro

Windows only. If checked, identify **vPro** (page 600)-enabled machines within the specified **Scan IP Range**. A machine does not need to be a vPro machine to discover vPro machines using LAN Watch. If a vPro machine is used as the LAN Watch discovery machine, it cannot discover itself.

**Note:** vPro configuration is a prerequisite to using this feature. Refer to the latest Intel documentation for information on how to configure vPro. At the time of this writing, the following link leads to the Intel documentation: <http://communities.intel.com/community/openportit/vproexpert> (<http://communities.intel.com/community/openportit/vproexpert>).

## Username / Password / Confirm

Enter the appropriate vPro credentials to return hardware asset details about vPro machines discovered during the LAN Watch. Typically the same credentials are defined for all vPro machines on the same LAN. The results are displayed using Agent > [View vPro](#) (page 69).

**Note:** vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using Remote Control > Power Management (page 377).

## Enable Alerts

If **Enable Alerts** is checked and a new device is discovered by LAN Watch, an alert is sent to all email addresses listed in **Email Recipients**. LAN Watch alerts and email recipients can also be specified using the Monitor > **Alerts** (page 219) page.

**Note:** Machines that have not been connected to the LAN for more than 7 days and then connect are flagged as new devices and will generate an alert.

## Email Recipients

If alerts are enabled, enter the email addresses where alert notifications are sent. You can specify a different email address for each managed machine, even if it is for the same event. The **From** email address is specified using System > **Outbound Email** (page 426).

## Ignore devices seen in the last <N> days

Enter the number of days to suppress alerts for new devices. This prevents creating alerts for devices that are connected to the network temporarily.

## Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Skip alert if MAC address matches existing agent

Checking this box suppresses alerts if the scan identifies that the MAC address of a network device belongs to an existing managed machine with an agent on it. Otherwise a managed machine that was offline for several days and comes back online triggers an unnecessary alert during a LAN Watch.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Agent

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### IP Range Scanned

The IP addresses that are scanned by the selected machine ID when LAN Watch runs.

### Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

### Primary DC

Windows only. If a primary domain controller icon  displays, this machine ID is a **primary domain controller** (page 596). If checked, performing a scan on a primary domain controller running Active Directory enables you to "harvest" the users and computers throughout a domain. You can subsequently install VSA agents automatically on computers listed in Active Directory and create VSA users and VSA users based on Active Directory administrator credentials. See **View AD Computers** (page 65) and **View AD Users** (page 66).

### SNMP Active

If the SNMP icon  displays, SNMP devices are included in the scheduled scan.

### vPro Active

Windows only. If the vPro icon  displays, vPro machines are included in the schedule scan.

### Alert Active

If checked  LAN Watch alerts are enabled for this scan.

---

## Install Agents

### Agent > Install Agents

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Install Agents** page installs the agent *on a remote system* and creates a new machine ID / group ID account. **Install Agents** remotely installs the packages created using **Deploy Agents** (page 39).

There are two methods of selecting machines to install agents on:

1. A list of machines is displayed on this page that have run **LAN Watch** (page 56). Clicking any LAN Watch machine—sometimes called the "discovery machine"—displays a listing of all discovered machines. Machines without an agent **display in red text**.
2. You can also install an agent by entering an IP address or host name that you know the discovery machine has access to, *even if its not listed on the page*.

**Note:** See System Requirements for a list of operating systems agents can be installed on.

### Using the Same Operating System for Discovery and Agent Installs

Windows, Macintosh, and Linux agents can discover Windows, Macintosh, and Linux machines on the same LAN using **LAN Watch** (page 56). Agent > **Install Agents** (page 60) can only install agents on:

- Windows machines if the LAN Watch discovery machine was a Windows machine.

- Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.
- Linux machines if the LAN Watch discovery machine was a Linux machine.

**Note:** Macintosh agent install packages require a credential when using **Agent > Install Agent**, or when installing agents using the `/s "silent install"` switch.

**Note:** For Linux machines, the `root` username alone—without a hostname or domain—must be used.

### Selecting Machines using LAN Watch

1. Run LAN Watch for a specific range of IP addresses using **Agent > LAN Watch** (page 56).

**Note:** None of the extra options in **LAN Watch** need be selected to list discovered machines on this page.

2. Select discovered machines in red text. They're the ones without an agent checking into this Kserver.

### Selecting a Machine using an IP or Host Name

- Enter the host name or IP address of a machine you know the discovery machine has access to, even if the machine is not listed on the page.

### Installing Agents on Selected Machines

1. Enter a administrator credential for the machines you've selected.
  - **If the target machine is on a domain, the administrator credential must include the domain.** The username field must be in the form `domain\administrator` or `administrator@domain`. If the target machine is not on a domain, then the administrator credential must include the hostname in the form `hostname\administrator`. For Linux machines, the `root` username alone—without a hostname or domain—must be used.
2. Select an agent install package. The selected agent install package must be appropriate for:
  - Windows machines if the LAN Watch discovery machine was a Windows machine.
  - Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.
  - Linux machines if the LAN Watch discovery machine was a Linux machine.
3. Click **Install**.

### Kconnect and SSH

The following technologies are used by **Agent > Install Agents** (page 60) to install agents on remote systems after a **LAN Watch** (page 56) scan is run on the discovery machine.

- Kconnect enables the installation of agent packages on remote target systems running a Windows operating system
- SSH (aka Secure Shell) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. This protocol is primarily used on Unix-based systems, including Mac OS X and Linux.
  - Mac OS X 10.3.9 and above machines must have **SSH Remote Login** in **System Preferences > Sharing > Remote Login** enabled to support the remote install of Macintosh agents using **Install Agents**.
  - On Linux `sshd` must be installed and enabled. This is not enabled by default in some Linux distributions.

A valid credential set with administrator rights is required to successfully install an agent remotely.

**Note:** The `KcsSetup` installer skips installation if it detects an agent is already on a machine if the `/e` switch is present in the installer package. The installer overwrites installation if it detects an agent is already installed on a machine if the `/r` switch is present in the installer package. The `/r` switch overrides the `/e` switch if both switches are included in the agent package.

### Running Kconnect

When **Install Agent** is run, `Kconnect.exe` is downloaded from the `KServer` into the `c:\kworking` directory and run using the following command line. You don't have to create this command line. **Install Agent** does it for you.

```
c:\kworking\kconnect \\hostname -u "adminname" -p "password" -c -f -d "c:\kworking\kcssetup.exe" > c:\kworking\LANInsAipAddr.txt
```

The terms `hostname` and `ipAddr` refer to the remote machine. If the agent is on a drive other than `C:` then the working files are referenced to the same drive the agent is installed on.

### Kconnect Error Messages

If a remote Windows agent installation fails for any reason, the `KServer` passes back the results reported by `Kconnect.exe`. Typically, `Kconnect.exe` is simply reporting OS errors that it received trying to execute a call.

### Typical Reasons for Install Failure

See **Install Issues and Failures** (page 45) for a general agent install issues and failures. *Additional* issues and failure related to remote installation of agents using **Install Agents** include:

- **File and Printer Sharing Not Enabled** - Verify File and Printer Sharing is enabled on the target machine's firewall if the target machine's firewall is on.
- **Blocked by Network Security Policy**
  - **Windows** - `Kconnect.exe` connects to the remote PC through the RPC service and runs as a local account. Remote access to this service is controlled by a Local or Domain **Security Setting**. Open **Local Security Policy** (part of Administrative Tools). Open **Local Policies\Security Options\Network access: Sharing and security model for local accounts**. The policy must be set to **Classic** for `Kconnect.exe` to operate across the network.

**Note:** Classic is the default setting for machines that are members of a domain. Guest is the default setting for machines that are not in a domain. Microsoft does not allow Windows XP Home Edition to become a domain member.

- **Macintosh** - SSH can be blocked by client management network policies, which are configured using **Server Admin** in Mac OS X 10.4 and later.
- **Failure to Connect** - The RPC service is not available on the target machine. For example, XP Home does not support RPC. This prevents anything from remotely executing on that box. On Windows XP you can turn this service on by opening Windows Explorer and selecting Tools - Folder Option... - View tab. Scroll to the bottom of the list and uncheck Use simple file sharing. The XP default configurations are as follows:
  - XP Pro on a domain - RPC enabled by default. Use simple file sharing is unchecked.
  - XP Pro in a workgroup - RPC disabled by default. Use simple file sharing is checked.
  - XP Home - RPC disabled always. Use simple file sharing is not available.
- **Network Path Not Found** - If you get a message saying that the network path could not be found, it means that the `admin$` share is not available on that machine. The `admin$` share is a default share that windows creates when it boots, it is possible to turn this off via the local security policy, or domain policy. If you want to check the shares on that remote machine you can use `Kconnect.exe` to retrieve a list for you. Type `kconnect \\ "net share"`. Check that the `admin$` share exists and points to `c:\windows` or `c:\winnt` on older operating systems.

- **Blocked by Anti-Virus Program** - Some anti-virus programs may classify Kconnect.exe and SSH as security threats and block its execution.
- **Invalid Credential** - The **credential** (*page 588*) must have administrator rights on the local machine. The agent requires administrator rights to install successfully.
  - **If the target machine is on a domain, the administrator credential must include the domain.** The username field must be in the form `domain\administrator` or `administrator@domain`. If the target machine is not on a domain, then the administrator credential must include the hostname in the form `hostname\administrator`. For Linux machines, the `root` username alone—without a hostname or domain—must be used.
  - On Vista, 7, and 2008 machines, ensure User Account Control (UAC) is disabled for the administrator rights credential being used.
  - **Mac OS** - Macintosh agent install packages **require** a credential when using Agent > Install Agent, or when installing agents using the /s "silent install" switch.
  - **Linux** - Linux machines credentials must use the `root` user on the **Install Agents** page. Embedding a `root` credential in the agent install package is unnecessary for Linux agent install packages used on the **Install Agents** page.
- **SSH Not Installed or Enabled** - Mac OS X 10.3.9 and above machines must have **SSH Remote Login** in **System Preferences > Sharing > Remote Login** enabled to support the remote install of Macintosh agents using **Install Agents**. On Linux `sshd` must be installed and enabled. This is not enabled by default in some Linux distributions.

## Testing and Troubleshooting

- **Kaseya KB article** (<http://community.kaseya.com/kb/w/wiki/how-can-i-troubleshoot-lan-watch-issues.aspx>).

## Admin Logon Name

The administrator name used to remotely access the selected machine. The **Admin Logon Name** must have administrator rights on the remote selected machine. Multiple accounts may have administrator rights on the same machine. Your domain administrator account may be different than the local administrator account. To ensure you are using the domain account enter the logon name using the `domain\administrator` or `administrator@domain` format. **If the target machine is on a domain, the administrator credential must include the domain.** For Linux machines, the `root` username alone—without a hostname or domain—must be used.

## Password

The password associated with the **Admin Logon Name**.

## Install

Click **Install** to schedule an installation of the selected install package on all selected machines.

## Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

## Select an Agent Package to Install

Select the agent package to remotely install on selected machines. These packages are created using **Deploy Agents** (*page 39*).

## Show all devices

Check this to see possible machines that did not report a host name. such as Mac machines that do not have a DNS.

## Agent

### Hide devices that match the MAC address of existing machine IDs

Check this box to hide all machines on a LAN with a [MAC address](#) (on page 592) matching the MAC address of an existing machine ID / group ID account.

### Hide devices that match the computer names of existing machine in <machine ID>

Check this box to hide machines that have a common computer name in this same group ID. A LAN Watch may discover an managed machine with a second device using a different MAC ID then the one used to report to the KServer. For example, the same managed machine may connect to the internet using direct connection and have a second wireless connection with a different MAC ID. Checking this box hides the second device from this list so that you don't assume you've found a new unmanaged machine.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Host Name

The host name of each device on the LAN discovered by the latest LAN Watch scan.

### IP Address

The private IP address of each device discovered by the latest LAN Watch scan.

### MAC Address

The [MAC address](#) (on page 592) of each device discovered by the latest LAN Watch scan.

### Vendor

The system manufacturer.

### Last Seen

The time each device was last detected by the latest LAN Watch scan.

---

## View LAN

### Client > View LAN

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [View LAN](#) page displays the results of the latest [LAN Watch](#) (*page 56*) scan run on a machine ID. Only machine IDs with returned scan data are available to select.

Click any machine ID to display a table listing all *machines* and *devices* found by LAN Watch run on that machine ID. Data only displays in the [host name](#) (on page 590) column for machines, not devices. Paging rows can be sorted by clicking column heading links.

### Host Name

The host name of each device on the LAN discovered by the latest LAN Watch scan. A host name only displays for computers. Hubs, switches, routers, or other network appliances do not return a host name.

### IP Address

The private IP address of each device discovered by the latest LAN Watch scan.

## MAC Address

The [MAC address](#) (on page 592) of each device discovered by the latest LAN Watch scan.

## Vendor

The system manufacturer.

## Last Seen

The time each device was last detected by the latest LAN Watch scan.

## SNMP Info

SNMP identifying information.

---

# View AD Computers

## Agent > View AD Computers

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [View AD Computers](#) page shows all computers listed in an [Active Directory](#) (page 583) when [LAN Watch](#) (page 56) runs on a system hosting Active Directory. Use [View AD Computers](#) to install agents automatically on computers listed in the Active Directory by policy at computer startup. Using this method has the following benefits:

- This policy ensures an agent is always present on a machine at every reboot, even if the agent is subsequently removed by a user.
- Agents can be deployed to an entire AD network even if the VSA user does not know the local credentials for each computer.
- A LAN Watch scan performed by an AD machine discovers all computers that are members of a domain, *whether the machines are online or not*.

**Note:** You must select a *Detail View* to see AD computers listed on this page.

## Switching From Summary View to Detail View

1. Select <All Groups> from the [Select Machine Group](#) drop-down to list all domain controllers that have run LAN Watch for *all machine groups you're authorized to access*.
2. Identify the machine groups and subgroups listed in the [Discovered By](#) column.
3. Select one of the machine groups or subgroups in Step 2 above from the [Select Machine Group](#) drop-down list to display a *details view* of domain controllers that are members of that machine group.

## Summary View

The summary view of [View AD Computers](#) lists all domain controllers that have run LAN Watch for *all machine groups you're authorized to access*.

## Discovered By

Lists the machine ID.group ID names of domain controllers that have performed a LAN Watch scan.

## Computers Found

Lists the number of computers, *with or without agents*, listed in the domain controller directory.

## Agent

### Agent Installed

Lists the number of computers *with agents* that are also listed in the domain controller's directory.

### Details View

The details view of [View AD Computers](#) displays computers listed in Active Directory services hosted on computers that have run LAN Watch *within a specified machine group*.

### Installing Agents on Active Directory Computers

You can associate an install package with an AD computer. This installs an agent package when the AD computer reboots, unless the agent is already installed. You can specify the agent package installed for each AD computer.

**Note:** See [Install Issues and Failures](#) (page 45) if an agent fails to install.

To associate an install package with an AD computer:

1. Check [Show Details](#) to display the [Canonical Name](#) (page 587) of discovered computers in the paging area.
2. Select an agent package from the [Select an Agent Package to install](#) drop-down list.
3. Click [Install Agent Policy](#).
4. Optionally click [Update Agent Policies](#) to copy a changed agent install package to the AD computer. The updated install package replaces the copy on the AD computer.
5. Optionally select an AD computer and click [Cancel](#) to un-associate an install package with an AD computer.

---

## View AD Users

### Agent > View AD Users

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [View AD Users](#) page lists all [Active Directory](#) (page 583) users discovered by [LAN Watch](#) (page 56) when [LAN Watch](#) runs on a system hosting Active Directory. Using [View AD Users](#):

- Agents can be automatically installed on each machine an Active Directory user logs onto.
- VSA users logons can be created based on Active Directory user logons.
- Portal Access logons can be created based on Active Directory user logons.
- Contact information can be extracted from Active Directory users and applied to the contact information for machine IDs.

**Note:** You must select a *Detail View* to see AD users listed on this page.

### Switching From Summary View to Detail View

1. Select <All Groups> from the [Select Machine Group](#) drop-down to list all domain controllers that have run LAN Watch for *all machine groups you're authorized to access*.
2. Identify the machine groups and subgroups listed in the [Discovered By](#) column.
3. Select one of the machine groups or subgroups in Step 2 above from the [Select Machine Group](#) drop-down list to display a *details view* of domain controllers that are members of that machine group.

## Summary View

The summary view of the [View AD Users](#) page lists all domain controllers that ran LAN Watch for *all machine groups you're authorized to access*.

### Discovered By

Lists the machine ID.group ID names of domain controllers that have performed a LAN Watch scan.

### Users Found

Lists the number of users contained in Active Directory found on a domain controller that ran LAN Watch.

### Assigned

Lists the number of [Users Found](#) whose contact information has been extracted from the Active Directory and assigned to a machine ID.

## Details View

The details view of [View AD Users](#) displays a list of Active Directory users on domain controllers that ran LAN Watch *within a specified machine group*.

### Installing Agents on Any Machine an AD User Logs Onto

You can associate an install package with an AD user. This installs an agent package on any machine a AD user logs onto, unless the agent is already installed. Even if the agent is subsequently removed from a machine, the agent will be re-installed the next time the AD user logs on. You can specify the agent package installed for each AD user.

**Note:** See [Install Issues and Failures](#) (page 45) if an agent fails to install.

To associate an install package with an AD user:

1. Select AD users listed in the [Logon Name](#) column of the paging area.
2. Select an agent package from the [Select an Agent Package to Install](#) drop-down list.
3. Click [Install Agent Policy](#).
4. Optionally click [Update Agent Policies](#) to copy a changed agent install package to the AD user's computer. The updated install package replaces the copy on the AD user's computer.
5. Select an AD user and click [Cancel](#) to un-associate an install package with an AD user.

### Creating VSA Users Based on AD Users

Create VSA users based on AD users. VSA users created using this method log onto the VSA using their AD domain, user name, and password. This means users only have to maintain credentials in a single location, the Active Directory.

**Note:** If a VSA user logon is based on an AD user, the VSA user's username and password cannot be changed within the VSA, only in Active Directory. Once usernames and passwords are changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep VSA logons updated with the latest changes to AD logons.

**Note:** An AD user can only be associated with *either* a VSA user logon or a machine user logon but *not both*.

To create a new VSA user based on an AD user:

1. Select an AD users listed in the [Logon Name](#) column of the paging area.

## Agent

2. Select a user role from the **Select User Role** drop-down list.
3. Select a scope from the **Select Scope** drop-down list.
4. Click **Create User**.

You can confirm the creation of the new VSA user using System > **Users** (page 397). VSA user names based on AD users are formatted as follows: <domainname>|<username>.

### Creating Portal Access Logons Based on AD Users

Create **Portal Access** logons based on an AD users. VSA users created using this method can log onto the VSA Portal Access menu using their AD domain, user name, and password. This means credentials only have to be maintained in a single location, the Active Directory.

**Note:** If a Portal Access logon is based on an AD user logon, the Portal Access username and password cannot be changed within the VSA, only in Active Directory. Once usernames and passwords are changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep Portal Access logons updated with the latest changes to AD logons.

**Note:** An AD user can only be associated with *either* a VSA user logon or a Portal Access machine but *not both*.

To create a new Portal Access logon based on an AD user:

1. Click the **unassigned** link for an AD user listed in the **Assigned To** column of the paging area.
2. Select a machine ID.group ID account in the popup window. The popup window closes.
3. Select the checkbox for this same AD user in the left most column.
4. Click **Create Machine Logon**.

You can confirm the creation of the new VSA user using Agent > **Portal Access** (page 81).

### Creating Staff Members Based on AD Users

Create staff member records based on AD users. If AD user information is changed, then the VSA updates the corresponding staff member record with the AD user information. This means user information only has to be maintained in one place, the Active Directory.

**Note:** If a VSA staff record is based on an AD user, the VSA staff record cannot be changed within the VSA, only in Active Directory. Once user information is changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep staff member records in the VSA updated with the latest changes in Active Directory.

To create new VSA Portal Access logon based on an AD user:

1. Select a department from the **Select Department** drop-down list.
2. Select the checkbox for an AD user in the left most column.
3. Click **Create Staff Member**.

You can confirm the creation of the new VSA user using System > Manage.

### Updating Contact Information for Machine IDs based on AD Users

If a machine ID is assigned to an AD user, then the VSA updates its own contact information for that machine ID with the latest contact information for that user in the Active Directory each time the user logs onto the machine ID. This enables users to update contact information once in the Active Directory and know the contact information for machine IDs in the VSA will be updated automatically.

**Note:** If a contact information is based on an AD user, the VSA staff record cannot be changed within the VSA, only in Active Directory. Once contact information is changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep contact information in the VSA updated with the latest changes in Active Directory.

To assign an AD user to a machine ID:

1. Click the **unassigned** link for an Active Directory user listed in the **Canonical Name** column of the paging area.
2. Select a machine ID.group ID account in the popup window. The popup window closes.

### Converting Your Existing VSA Logon to use your Domain Logon

You can convert your own VSA logon to use your domain logon as follows:

1. Open the System > **Change Logon** page in the VSA.
2. Enter your current VSA password in the **Old Password** field.
3. Enter you domain and domain logon name, formatted *all in lowercase* using the format domain/username, in the **Username** field.
4. Enter your domain password in the **New Password / Confirm Password** fields.

This enables you to logon to the VSA using your domain logon and have your VSA logon name and password managed using Active Directory. At the same time, you can continue to use all your previous VSA share rights, procedures and other user settings.

**Note:** If a VSA user logon is based on an AD user, the VSA user's username and password cannot be changed within the VSA, only in Active Directory. Once usernames and passwords are changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep VSA logons updated with the latest changes to AD logons.

---

## View vPro

### Agent > View vPro

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **View vPro** page displays hardware information about vPro-enabled machines discovered while running **LAN Watch** (page 56). This information is only available if a machine's vPro credential is specified by the **LAN Watch**.

Types of hardware information returned by the vPro machine include:

- Agent check-in status, if the vPro machine has an agent installed
- Computer Information
- Motherboard Asset Information
- BIOS Information
- Processor Information
- RAM Information
- Hard Drive Information

**Note:** vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using **Remote Control > Power Management** (page 377).

**Note:** A vPro-enabled machine can be booted up using an ISO file using Remote Control > Remote ISO Boot (page 378).

**Intel vPro Rebate** - Kaseya is participating in a vPro rebate program offered by Intel. If you have installed vPro enabled machines and perform a LAN Watch—and the vPro machine qualifies for the rebate—you can quickly generate the information you need by clicking the **Generate Intel® vPro™ rebate file** button. This generates a .CVS file containing the information you need document your rebate claim with Intel. An **Intel® vPro™ Technology Activation Rebate Rules** link is also provided.

---

## Copy Settings

### Agent > Copy Settings

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Copy Settings** page copies selected settings from a single source machine ID to multiple machine IDs. You can copy settings *from only one source* machine ID or template at a time. But you can copy different types of settings from different source machine IDs or templates in succession.

### Copy Settings and Templates

**Machine ID templates** (page 592) are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > **Copy Settings** to copy these changes to any number of machines IDs you are authorized to access. Be sure to select **Do Not Copy** for any settings you do not want to overwrite. Use **Add** to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

### Copy

Click **Copy** to select a source machine. Once you select the source machine a second window displays the types of settings you can copy.

By selecting only certain types of settings to copy, you can avoid overwriting customer specific settings you want to keep, such as the **Patch File Source**, which is different for each customer.

Select the **Add** option to add settings to target machines without replacing existing settings.

The types of agent settings you can copy include:

- Credential
- Agent Menu
- Checkin Control
- Working Directory
- Logs
- Machine Profile - Refers to settings in Audit > **Edit Profile** (page 79).
- View Collections
- Portal Access
- Remote Control Policy
- Patch Settings

- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These all the alert types on the Monitor > [Alerts](#) (page 219) page except for Event Log alerts and System alerts.
- Event Log Alerts - Includes copying [Event Log Settings](#) (page 37).
- Monitor Sets
- Distribute Files
- Protection
- Agent Procedure Schedules

### Select Machine ID

Click the [Select Machine ID](#) link to specify which machine ID to copy settings from.

### Spread agent procedure schedules when copying to multiple machines

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10,

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Status

Shows the machine name that settings were copied from and the time they were copied.

---

## Import / Export

### Agent > Import / Export

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Import / Export](#) page imports and exports machine ID account settings as XML files, including scheduled agent procedures, assigned monitor sets and event sets. Log data is not included in the

import or export. You can use [Import / Export](#) to migrate machine ID account settings, including [machine ID templates](#) (page 592), from one KServer to the next.

**Note:** See [Copy Settings](#) (page 70) for a list of the types of settings associated with a machine ID account.

**Note:** For the latest instructions on migrating an existing KServer to a new machine see [Moving the Kserver](#) section in the the KB article [latest Kserver installation and upgrade user guide](#) ([help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp](http://help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp)).

**Note:** Sample templates for specific types of machines can be imported and are available on the [Kaseya forum](#) in our [Kaseya Connections website](#) at <http://community.kaseya.com> (<http://community.kaseya.com>).

### To Export Machine ID Settings

1. Click the [select the machine](#) link. A machine selection dialog box displays.
2. Optionally filter the display of the machine IDs listed using the [machine ID / group ID filter](#) (page 592).
3. Click a machine ID link to export. The machine ID you selected now displays on the [Import / Export](#) page.
4. Click [Export](#). The page displays an XML statement of the agent settings being exported.
5. Export the XML statement by:
  - Copying the XML text to the clipboard.
  - Right-clicking the [Download](#) link and selecting the [Save Target As](#) option to save the XML text as an XML file on your local computer.

### To Import Machine ID Settings

1. Click [Browse](#) to select an XML file representing the settings of a machine ID account. Typically these XML files are created by exporting them from another KServer.
2. Click [Import](#). A set of additional options displays.
3. Accept or specify the name of the machine ID. A new one is created if this name doesn't already exist in the KServer.
4. Accept or select a different group ID.
5. Optionally check the box next to [Replace existing data if this machine ID already exists](#).
6. Optionally change the email notification address for all alerts defined for this machine ID account.
7. Click [Finish](#) to complete the import.

---

## Suspend

### Agent > Suspend

- This page applies to the following products: [On Premises](#), [Kaseya Advanced](#), [Kaseya Essentials](#), [IT Center](#), [IT Workbench](#)

The [Suspend](#) page suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings. When suspended, a machine ID displays a suspended icon  next to it. While a machine ID account is suspended the managed machine displays a gray agent icon  in the [system tray](#) (on page 599).

You can filter the display of machine IDs on any agent page using the [Show machines that are suspended/not suspended](#) option in [View Definitions](#) (page 28).

### Suspend

Click [Suspend](#) to suspend agent operations on selected machine IDs.

## Resume

Click [Resume](#) to resume agent operations on selected machine IDs.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Suspended

Displays `Suspended` if the machine ID is suspended.

---

# Agent Menu

### Agent > Agent Menu

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The [Agent Menu](#) page specifies the options that display in the agent menu of a user's machine. The user displays the agent menu by right-clicking the agent icon  in the [system tray](#) (on page 599) of the managed machine. This page can also *prevent* the agent icon  from displaying on the user's machine. Changes made using this page take effect at the next agent check-in and display **in red text** until then.

**Note:** See [Agent Icons](#) (page 25) for a general explanation of how agent icons display on the user's machine.

## Hiding the Agent Icon on the User's Machine

To hide the agent icon altogether:

1. Select one or more machine IDs.
2. Uncheck the [Enable Agent Icon](#) checkbox.
3. Click [Update](#).

All of the other checkbox settings will become dimmed, indicating that all agent menu options have been disabled.

### Preventing the User from Terminating the Agent Service on the User's Machine

If the **Exit** option is enabled on a user's managed machine, the user can terminate the agent service on the managed machine by selecting this option. When the agent service is stopped, the managed machine becomes invisible to VSA users and can no longer receive commands from the KServer.

To remove the **Exit** option from agent menus on managed machines:

1. Select one or more machine IDs.
2. Uncheck the **Exit** checkbox.
3. Click **Update**.

### Checkboxes

- **Enable Agent Icon** - Check to display the agent icon in the system tray of the managed machine. Uncheck to hide the agent icon and prevent the use of agent menu options.
- **About <Agent>** - Check to enable the machine user to click this option to display the About box for the installed agent. The default option label `Agent` can be customized.
- **<Contact Administrator...>** - Check to enable the machine user to click this option to display either the user's **Portal Access** (page 596) page or a different contact URL. The default option label `Contact Administrator...` can be customized.
- **<Your Company URL...>** - Check to enable the machine user to click this option to display the URL specified in the corresponding URL field.
- **Disable Remote Control** - Check to enable the machine user click this option to *disable* remote control on the user's managed machine.
- **Set Account...** - Check to enable the machine user to click this option to display their machine ID.group ID.organization ID and change the KServer address the agent checks into.
- **Refresh** - Check to enable the machine user to initiate an immediate **full check-in** (page 588).
- **Exit** - Check to enable the machine user to terminate the agent service on the managed machine.

### Update

Click **Update** to apply agent menu settings to selected machine IDs.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## ACObSRx

This column summarizes the agent menu options enabled for a machine ID. **ACObSRx** applies to the keyboard shortcuts that are used to access each option in the agent menu.

A letter indicates that option displays in the agent menu. A "-" indicates that menu option does not display in the agent menu.

**A** = About Agent

**C** = Contact User

**O** = Launches the URL specified in the URL field. The agent displays the text listed in the field to the left of the URL field.

**b** = Disable Remote Control

**S** = Set Account...

**R** = Refresh

**x** = Exit

## About Title

The text appended to the label for the **About** option on the agent menu. For example, if the About Title is `Agent` then the label of the **About** option displays as `About Agent`.

## Contact Title

The text displayed on the agent menu for contacting a VSA user.

## Custom Title

The text displayed on the agent menu for contacting a custom URL.

## Contact URL

The URL to display when the `Contact Administrator...` option is selected by the machine user. The default URL is the **Portal Access** (*page 81*) page. A different URL can be entered.

## Custom URL

The URL to display when this agent menu option is selected by the user.

---

# Check-In Control

## Agent > Check-In Control

- This page applies to the following product: *On Premises*

The **Check-In Control** page specifies when and where each agent should check in with a KServer. Changes made using this page take effect at the next agent check-in and display **in red text** until then. You can specify the primary and secondary KServer names/IP addresses used by the agent to check in, the bandwidth consumed by an agent to perform tasks and the check-in period.

**Note:** The primary and secondary KServer values and the minimum and maximum check-in periods are subject to the policies set using **System > Check-in Policy** (*page 393*). This prevents users from selecting settings that place undue stress on servers running the KServer service.

**Note:** **Check-in Control** information can also be maintained using the **Agent Settings** tab of the **Live Connect** (*page 54*) and **Machine Summary** (*page 137*) pages.

## Migrating Agents from one KServer to Another

You may decide for performance or logistical reasons to migrate managed machines to a new KServer. This can be done at any time, whether or not the agents are currently checking in.

1. At the **original** KServer, set the **primary** KServer setting to point to the **new** KServer address.
2. At the **original** KServer, point the **secondary** KServer setting to the **original** KServer.
3. At the **new** KServer, set both the **primary** and **secondary** KServer to point to the **new** KServer.
4. Wait for all the agents to successfully check into the **new** KServer. At that time, the **original** KServer can be taken off-line.

**Note:** For the latest instructions on migrating an existing KServer to a new machine see [Moving the KServer section in the the KB article latest Kserver installation and upgrade user guide \(help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp\)](http://help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp).

## Changing the Port used by Agents to Check into the KServer

1. Set the **Primary** Port to the **new** port.
2. Set the **Secondary** Port to the **old** port.
3. Wait for the new settings to take effect on all the agents.
4. Display the System > **Configure** (*page 412*) page. Enter the new port number in the **Specify port Agents check into server with** edit box and click the **Change Port** button.

**Note:** If any agents have not migrated to the new port before you switch the KServer, you will have to manually change the port at the managed machine. Right click the agent icon  in the system tray to display the agent menu on the managed machine and select the **Set Account...** option. Enter the server address and port. For example, 192.168.1.7:1234.

## Primary KServer

Enter the IP address or fully qualified **host name** (on page 590) of the machine ID's primary KServer. This setting is displayed in the **Primary KServer** column.

Kaseya agents initiate all communication with the KServer. For this reason the agents must always be able to reach the domain name or IP (Internet Protocol) address assigned to the KServer. Choose an IP address or domain name which can be resolved from all desired network(s), both on the local LAN and across the internet.

**Best Practices:** Although a public IP address may be used, Kaseya recommends using a **domain name server (DNS)** name for the KServer. This practice is recommended as a precaution should the IP address need to change. It is easier to modify the DNS entry than redirecting orphaned agents.

## Primary Port

Enter the port number of either the primary KServer or a virtual system server. This setting is displayed in the **Primary KServer** column.

**Warning:** Do NOT use a *computer name* for your server. The agent uses standard WinSock calls to resolve a fully qualified **host name** (on page 590) into an IP address, which is used for all agent connections. Resolving a computer name into an IP address is done by NETBIOS, which may or may not be enabled on each computer. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

## Secondary KServer

Enter the IP address or fully qualified host name of the machine ID's secondary KServer. This setting is displayed in the [Secondary KServer](#) column.

## Secondary Port

Enter the port number of either the secondary KServer or a virtual system server. This setting is displayed in the [Secondary KServer](#) column.

## Check-In Period

Enter the time interval for an agent to wait before performing a [quick check-in](#) (page 588) with the KServer. A check-in consists of a check for a recent update to the machine ID account. If a recent update has been set by a VSA user, the agent starts working on the task at the next check-in. This setting is displayed in the [Check-In Period](#) column. The minimum and maximum check-in periods allowed are set using System > [Check-in Policy](#) (page 393).

**Best Practices:** The agent maintains a persistent connection to the KServer. As a result, quick check-in times do not effect response times from the agent. The quick check-in time sets the maximum time to wait before re-establishing a dropped connection. Setting all your machine's quick check-in time to 30 seconds guarantees each agent recovers from a dropped connection within 30 seconds, assuming connectivity is successful.

## Bind to Kserver

If checked, the agent is bound to a [unique Kserver ID](#). Bound agents cannot check-in successfully unless the unique Kserver ID they are bound to using the Agent > [Check-in Control](#) (page 75) page matches the unique ID assigned to the KServer using the System > [Configure](#) (page 412) page. A lock  icon in the paging areas shows the agent is bound. To *unbind* agents, select machines IDs, ensure [Bind to Kserver](#) is unchecked and click [Update](#). The lock  icon no longer displays for selected machines.

## Bandwidth Throttle

Limit the agent to consuming a maximum amount of bandwidth on the system with this control. By default the agent shares bandwidth with all other running applications so you typically do not need bandwidth throttle enabled. Disable bandwidth throttle by entering a 0.

## Warn if multiple agents use same account

The KServer can detect if more than one agent is connecting to the KServer and using the same machine ID.group ID.Organization ID. This problem could be caused by installing an agent install package pre-configured with the machine ID on more than one machine. Check this box to receive notifications of more than one agent using the same account each time you log into the KServer as a user.

## Warn if agent on same LAN as KServer connects through gateway

If you are managing machines that share the same LAN as your KServer then you may get this alert. By default all agents connect back to the KServer using the [external name/IP address](#) (page 412). TCP/IP messages from these agents travel through your internal LAN to your router, and then back to the KServer. Some routers do a poor job of routing internal traffic back through themselves. Check this box to receive a notification when the KServer detects an agent may be on the same LAN but connecting through the router.

**Note:** Agents on the same LAN as the KServer should specify the internal IP address shared by both the agent and the KServer on the [Check-In Control](#) (page 75) page.

## Agent

### Update

Click [Update](#) to update all selected machine IDs with the options previously selected.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

---

## Working Directory

### Agent > Working Directory

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Working Directory](#) page sets the path to a directory on the managed machine used by the agent to store working files.

Depending on the task at hand, the agent uses several additional files. The server transfers these files to a working directory used by the agent on the managed machine. For selected machine IDs you can change the default working directory from C:\kworking to any other location.

**Warning:** Do not delete files and folders in the working directory. The agent uses the data stored in the working directory to perform various tasks.

You can approve this directory in security programs, such as virus checkers, to allow operations such as remote control from being blocked.

**Note:** A working directory can also be maintained using the [Agent Settings](#) tab of the [Live Connect](#) (page 380) and [Machine Summary](#) (page 137) pages. A working directory can be written to using a [Get Variable](#) command in agent procedures.

### Set

Click [Set](#) to set selected machine IDs use the working directory previously entered.

## Set a path to a directory used by the agent to store working files

Enter the path of the working directory used by the agent on the managed machine.

## Set as System Default

Click [Set as System Default](#) to set a system-wide default for the agent working directory. This option only displays for [master role users](#) (page 600).

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Working Path

The path of the working directory assigned to this machine ID. On a Mac OS X system, if the path name contains a space, then it must be preceded with a backslash. For example: `/tmp/name\ with\ three\ spaces`

---

# Edit Profile

## Agent > Edit Profile

- This page applies to the following products: [On Premises](#), [Kaseya Advanced](#), [Kaseya Essentials](#), [IT Center](#), [IT Workbench](#)

The [Edit Profile](#) page maintains contact information, the language preference for the agent menu on the user's machine and notes about each machine ID/group ID account. Profile information can be maintained in three other places:

- The contact information in the [Edit Profile](#) page can be automatically populated when a new account is created using the Agent > [Create](#) (page 49) page.
- VSA users and machine users can both maintain contact information using the Home > [Change Profile](#) tab in the [Live Connect](#) (page 380) or [Portal Access](#) (page 81) window.
- VSA users only can maintain notes and contact information using the [Agent Settings](#) tab of the [Live Connect](#) (page 380) and [Machine Summary](#) (page 137) pages.

To change user accounts settings:

## Agent

1. Select a machine ID in the paging area.
2. Enter **Notes**, **Admin Email**, **Contact Name**, **Contact Email** and **Contact Phone** information.
3. Press **Update**.

## Notes

Enter any notes about a machine ID account. Helpful information can include the machine's location, the type of machine, the company, or any other identifying information about the managed machine.

## Show notes as tooltip

If checked, **Edit Profile** notes are included as part of the tooltip that displays whenever the cursor hovers over a machine ID's **check-in status icon** (see "**Check-in Status**" on page 588).

## Auto assign tickets

Auto assign a ticket to this machine ID if the **Ticketing email reader** (page 449) receives an email from the same email address as the **Contact Email**. Applies when new emails come into the ticketing email reader that do not map into any of the **email mappings** (page 451).

**Note:** if multiple machine IDs have the same contact email, then only one machine ID can have this checkbox checked.

## Contact Name

Enter the name of the individual using the managed machine. This setting is displayed in the **Contact Name** column.

## Contact Email

Enter the email address of the individual using the managed machine. This setting is displayed in the **Contact Email** column.

## Contact Phone

Enter the phone number of the individual using the managed machine. This setting is displayed in the **Contact Phone** column.

## Admin Email

Enter the email address providing administrator support for this managed machine. This setting is displayed in the **Admin Email** column.

## Language Preference

The language selected in the **Language Preference** drop-down list determines the language displayed by an **agent menu** (page 73) on a managed machine. The languages available are determined by the language packages installed using System > **Preferences** (page 391).

## Machine Role

The machine role to apply to selected machine IDs. **Machine roles** (page 403) determine the **Portal Access** (page 81) functions available to the machine user.

## Update

Click **Update** to update selected machine IDs with the profile information previously entered.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

---

# Portal Access

## Agent > Portal Access

- This page applies to the following product: On Premises

The [Portal Access](#) page defines the logon name and password, by machine ID, required to use [Live Connect](#) (page 380) as a machine user *remotely*. A [Live Connect](#) session run by a machine user is called [Portal Access](#). The functions displayed using [Portal Access](#) are determined by the System > Machine Roles > [Access Rights](#) (page 403) tab.

**Note:** You can download a Live Connect PDF from the first topic of online help.

**Note:** See [Enabling Ticketing for Portal Access Users on Unsupported Browsers](#) (page 82).

## Accessing Portal Access Locally

Machine users do not have to logon to [Portal Access](#) locally. Clicking the agent icon in the system tray of their machine initiates the [Portal Access](#) session without having to logon.

## Accessing the Portal Access Logon Page Remotely

A machine user can display the [Portal Access](#) logon page for their own machine from another machine as follows:

1. Browse to the `http://your_KServer_address/access/` page, substituting the appropriate target KServer name for `your_KServer_address` in the URL text.

**Note:** This is the same page that VSA users use to logon to the VSA.

2. Logon by entering the user name and password assigned to the machine ID. The user name and password is specified using the Agent > [Portal Access](#) page.

The [Portal Access](#) page displays. The machine user can click any menu option as though he or she were logged in from their own managed machine. The machine user can click the [Desktop](#) or [File](#)

## Agent

**Transfer** menu options to initiate a remote connection to their own machine, create or view ticket, or initiate a chat, if these options are enabled by machine role.

### Re-Enabling User Logons

Machine user logons follow the same **Logon Policy** (page 425) as VSA user logons. If a user attempts to logon too many times with the wrong password their account will automatically be disabled. You can re-enable the logon by setting a new password or waiting for the disable account time to lapse.

### Customizing Portal Access

**Portal Access** sessions can be customized using System > Customize > **Live Connect** (page 432), including adding a logo, welcome page and links to other URLs.

### Logon Name

Enter the **Logon Name** the user must use to log into the VSA to initiate chat sessions, enter or view tickets and/or get remote access to their machine. Logon names and passwords are case sensitive. Passwords must be at least six characters long. The **Logon Name** defaults to the machineID.groupID name.

### Create Password, Confirm Password

Define a password for the machine user logon. Passwords must be at least 6 characters long. The machine user can change the password after the VSA user assigns one.

### Apply

Click **Apply** to apply the **Portal Access** logon name and password to the selected machine ID.

### Clear

Permanently remove the **Portal Access** logon **credential** (page 588) from the selected machine ID.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Logon Name

The **Portal Access** logon name assigned to this machine ID.

### User Web Logon

Displays **Enabled** if a **Portal Access** logon name and password has been assigned to this machine ID. Indicates that a machine user can log into the **Portal Access** page for their own machine *remotely* using a web browser on any other machine.

## Enabling Ticketing for Portal Access Users on Unsupported Browsers

**Live Connect** and **Portal Access** are not supported on certain browsers, such as browsers older than IE8 or Firefox 3.5. Machine users required to work with unsupported browsers can be enabled to create and view **Ticketing** (page 435) tickets as follows:

1. Create a separate machine role for unsupported browser users in System > **Machine Roles** (page 403). For example, create a **Tickets Only** machine role.
2. For the new machine role you just created, uncheck the **Live Connect** checkbox in the System > Machine Roles > **Access Rights** (page 403) tab.
3. Assign machines with unsupported browsers to this new machine role.

4. When machine users click their agent icon, a single **Ticketing** window displays instead of the **Portal Access** window.

**Note:** Enabling this option applies to all users using the same managed machine.

---

## Set Credential

### Agent > Set Credential

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Set Credential** page registers the credential required by an agent to perform user level tasks on a managed machine. A credential is the logon name and password used to authenticate a user or process's access to a machine or network or some other resource. Most agent tasks do not require a credential. Credentials are specifically required or referenced by the following:

- **Patch Management** - If a credential is defined for a machine ID, then **Patch Management** installs all new patches using this credential. Therefore, **Set Credential** (page 83) should always be a user with administrator rights.
- **Patch Status** (page 312) - Patch Status resets test results every time a machine ID's **Set Credential** changes.
- **File Source** (page 340) - File Source may require a set credential be defined for the machine ID acting as the file share.
- **Patch Alert** (page 342) - Set up an alert to notify you if a machine ID's credential is missing or invalid.
- **Office Source** (page 346) - The agent must have a credential to access the alternate Office source location, in case a patch is being installed when no user is logged into the machine.
- **If-Then-Else** (page 97) - The `Use Credential` command in the agent procedure editor requires a credential be defined in **Set Credential** to run successfully.
- **Image Location** - If a UNC path is specified in **Image Location**, a credential must be defined using **Set Credential** that provides access to this UNC path. Without the credential, the machine will *not* have access to the image location and the backup will fail.
- **View Definitions** (page 28) - Includes a **Machines with Credential status** option that allows you to filter the display of machine IDs on any agent page by their credential status.
- **Desktop Policy and Migration** - Installing the client for this module requires a credential be defined.

### Blank Passwords

Blank passwords can be used if the managed machine's **Local Security Policy** allows blank passwords. On the managed machine, open the Local Security Policy tool in Administrative Tools. Navigate to Local Policies - Security Options. Look for a policy named `Accounts: Limit local account use of blank passwords to console logon only`. The default setting is enabled. Change it to disabled and a credential with a blank password will work.

### Username

Enter the username for the credential. Typically this a user account.

### Password

Enter the password associated with the username above.

### Domain

**Local user account** - Select this option to use a credential that logs into this machine locally, without reference to a domain.

## Agent

**Use machine's current domain** - Create a credential using the domain name this machine is a member of, as determined by the **latest audit** (*page 587*). This makes it easier to **Select All** and rapidly set a common username/password on multiple machines, even if selected machines are members of different domains.

**Specify domain** - Manually specify the domain name to use for this credential.

## Apply

Assign the credential to all checked machine IDs. Machine IDs with assigned credentials display the username and domain in the associated table columns.

## Clear

Remove the credential from all checked machine IDs.

## Test

Click **Test** to verify whether a username/password/domain credential will work before assigning it to a machine ID.

## Cancel

Click **Cancel** to cancel the testing of a username/password/domain credential.

---

# Update Agent

## Agent > Update Agent

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Update Agent** page schedules managed machines to be updated with the latest version of the agent software at the agent's next check-in. Updating the agent software makes no changes to the **agent settings** (*page 583*) you have defined for each agent.

## Update Agent

Click **Update Agent** to schedule selected machines to be updated.

## Remind me at logon when agents need an update

If checked, a popup window displays when VSA users logon if managed machines under their control need to be updated with the latest version of the agent software. The reminder only displays if at least one agent within the VSA user's **scope** (*page 404*) requires updating. Users can disable this feature at logon time and can re-activate it by selecting this checkbox.

## Force update even if agent is at version x.x.x.x

If checked, machines selected for update are updated with new files to replace the agent files on the managed machine, even if the agent version is currently up to date. This performs a "clean" installation of the agent files.

## After update run agent procedure <select agent procedure>

Select an agent procedure to run immediately after an agent update completes. This capability lets you re-apply customizations to an agent that may be lost after an agent update. Typically these customizations involve hiding or renaming agent identifiers on managed machines so as to prevent users from recognizing the agent is even installed.

## Cancel Update

Click [Cancel Update](#) to cancel a pending update on selected managed machines.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Agent Version

The version of the agent software running on the managed machine. **Version numbers in red** indicate that the version on the agent machine is not the same as the latest version available.

## Update Agent Procedure

The agent procedure assigned to run when the agent is updated.

## Last Update

The date the agent was last updated on the managed machine. Since the server must wait for the managed machine to check-in, according to the check-in schedule as specified in Agent > [Check-In Control](#) (page 75), *Pending* displays in the [Last Update](#) column until the next check-in occurs.

---

# File Access

## Agent > File Access

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [File Access](#) page prevents unauthorized access to files on managed machines by rogue applications or users. Any application can be approved or denied access to the file.

**Note:** You may also block operating system access to the protected file by blocking access to `explorer.exe` and/or `cmd.exe`. This prevents the file from being renamed, moved, or deleted therefore completely locking down the file from tampering.

## Agent

### Multiple Agents

If **multiple agents** (page 45) are installed on a machine, only one agent at a time controls the drivers required to use **File Access** (page 85), **Network Access** (page 87), **Application Blocker** (page 89). These functions can only be performed by the agent controlling these drivers.

### Block

To protect a file from access by rogue applications, enter the filename and click the **Block** button. This displays the **File Access** popup window.

The dialog presents the user with one of the following options:

- **Filename to access control** - Enter the **file name and/or a portion of the full path**. For example, adding a file named `protectme.doc` to the list, protects occurrences of `protectme.doc` in any directory on any drive. Adding `myfolder\protectme.doc` protects all occurrences of the file in any directory named `myfolder`.
- **New** - Add in a new application to the access list. You can manually enter the application or use the **Search...** button to select an application name.
- **Remove** - Removes an application from the approved access list
- **Search** - Select a machine ID to search the list of applications installed on that machine ID and select an application name. This list is based on the latest audit performed on that machine ID. You are not actually browsing the managed machine.
- **Ask user to approve unlisted** - Lets users approve/deny access to the file on a per application basis each time a new application tries to access that file. Use this feature to build up an access control list based on normal usage.
- **Deny all unlisted** - Blocks an application from accessing the file. Select this option if you are already sure of which files need access and which do not.

### Unblock

Remove an application from the protection list by clicking the **Unblock** button. This opens a new dialog box listing all protected files for the selected machine IDs. You can remove files from just the selected machine or from all machines containing that file path.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Filename

Filename of the file to be blocked. Click the edit icon  next to any filename to change file access permissions for that filename.

## Approved Apps

Lists applications approved to access the file on the machine ID.

## Ask User Approval

If checked, the user of a machine ID is asked to approve file access if an unapproved application attempts to access the file.

---

# Network Access

## Agent > Network Access

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Network Access** page lets you approve or deny **TCP/IP-protocol-based network access** on a per application basis. Users can also be notified when an unlisted application accesses the network, permitting or denying that application network access. Typically this function is used to control access to internal and external *internet* sites, but can include internal LAN traffic that also uses the TCP/IP protocol.

## Driver

This function requires the driver be *enabled* to block network access and monitor network bandwidth statistics. *The driver is disabled by default.* This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. *An enabled driver only takes effect after a reboot of the machine.*

**Note:** To determine which applications should be approved or denied network access, use the **Network Statistics** (page 155) report to view network bandwidth utilization versus time. Drill down and identify peak bandwidth consumers by clicking the graph's data points. See which application and which machine use bandwidth at any point in time.

**Warning:** Applications that do not use the Windows TCP/IP stack in the standard way may conflict with the driver used to collect information and block access, especially older legacy applications.

## Multiple Agents

If **multiple agents** (page 45) are installed on a machine, only one agent at a time controls the drivers required to use **File Access** (page 85), **Network Access** (page 87), **Application Blocker** (page 89). These functions can only be performed by the agent controlling these drivers.

## To approve or deny network access to one or more applications

1. Check the checkbox next to one or more machine IDs in the **Machine.Group ID** column.
2. Click the link of *any* machine ID in the **Machine.Group ID** column. It does not have to be the machine ID you checked. This displays the **Application List** popup window, listing all applications installed on that machine ID. The list is based on the latest audit that was performed for that machine ID.
3. Since the list in the **Application List** window may be large, you can control the applications displayed by clicking **Filter** to filter the list.
4. Check the checkboxes next to the application name you wish to approve or deny network access to.

## Agent

5. You can also enter application names in the **Add applications not found by audit here** edit field, to identify applications not listed.
6. Click the **Select** button to confirm your selections and close the **Application List** window. The selected applications now display at the top of the page.
7. Click **Approve Apps** or **Deny Apps**. The applications selected in the **Application List** window are added from the **Approved Apps/Denied Apps** column.

### To remove approve and deny settings for one or more machine IDs

1. Check the checkbox next to one or more machine IDs in the **Machine.Group ID** column.
2. Click the **Remove Apps** button.

### Network Access Options

- **Notify user when app blocked** - Notify the user when a blocked application attempts to access the network. Use this function to build up the access list based on normal usage. This lets you see which applications on your system are accessing the network and when. The machine user is prompted to select one of four responses when an application is blocked:
  - **Always** - Allows the application access to the network indefinitely. Users will not be prompted again.
  - **Yes** - Allows the application access to the network for the duration of the session. Users will be prompted again.
  - **No** - Denies the application access to the network for the duration of the session. Users will be prompted again.
  - **Never** - Denies the application access to the network indefinitely. Users will not be prompted again.
- **Enable/Disable driver at next reboot - Enable/Disable** the network access protection driver for an agent. Applications that do not use the Windows TCP/IP stack in the standard way may conflict with this driver, especially older legacy applications. **The agent can not monitor network statistics or block network access if this driver is disabled.** *An enabled driver only takes effect after a reboot of the machine.*
- **Apply Unlisted Action** - An unlisted application is one that has not been explicitly approved or denied access to the network. Select the action to take when an unlisted application attempts to access the network.
  - **Ask user to approve unlisted** - A confirmation dialog box displays if an unlisted application attempts to access the network.
  - **Approve all unlisted** - The unlisted application is granted access to the network.
- **Deny all unlisted** - The unlisted application is denied access to the network and the application is closed on the managed machine.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline

-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Notify User

A green checkmark  in the **Notify User** column indicates that the managed machine user is notified when an application attempts to access the network that has been denied network access.

To notify the user when a application has been denied:

1. Select machine IDs.
2. Click the **Enable** button for **Notify user when app is blocked**.

To remove this notification:

1. Select machine IDs that display a green checkmark  in the **Notify** column.
2. Click the **Disable** button for **Notify user when app is blocked**.

## Enable Driver

Identifies on a per machine ID basis, which machines have the network protection driver enabled or not. *An enabled driver only takes effect after a reboot of the machine.*

## Unlisted Action

Displays the **Unlisted Action** to take when an unlisted application attempts to access the network. See **Apply Unlisted Action** above.

## Approved Apps / Denies Apps / Remove Apps / Remove All

These settings can only be applied once the driver is enabled.

- Approved applications are listed in the first row.
- Denied applications are listed in the second row.
- If the **Approve all unlisted** radio option is selected and applied to a machine ID, then the approved application list is replaced by the phrase `Approve All Unlisted`.
- If **Deny all unlisted** radio option is selected and applied to a machine ID, then the denied application list is replaced by the phrase `Deny All Unlisted`.
- Click **Remove Apps** to remove a selected applications from selected machines.
- Click **Remove All** to remove all applications from selected machines.

---

# Application Blocker

## Agent > Application Blocker

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Application Blocker** page prevents any application from running on a machine ID. Blocked applications cannot be renamed, moved, or deleted from the system.

## Multiple Agents

If **multiple agents** (page 45) are installed on a machine, only one agent at a time controls the drivers

## Agent

required to use [File Access](#) (page 85), [Network Access](#) (page 87), [Application Blocker](#) (page 89). These functions can only be performed by the agent controlling these drivers.

## Block

To block an application from running on a machine:

1. Select one or more machine IDs. Only machine IDs currently matching the [Machine ID / Group ID filter](#) (page 26) are displayed.
2. Enter the application's filename in the edit box.

The application can be [referenced by file name and/or a portion of the full path](#). For example, adding an application named `blockme.exe` to the list, prevents all occurrences of `blockme.exe`, on any directory or on any drive, from running. Adding `myfolder\blockme.exe` prevents occurrences of the application in any directory named `myfolder` from running.

3. Click the **Block** button.
4. The blocked application displays in the [Application](#) column beside the selected machine IDs.

## Unblock

To unblock an application from the blocked list:

1. Select one or more machine IDs that show blocked applications in the [Application](#) column.
2. Click the **Unblock** button. This opens a [File Access](#) popup window listing all blocked applications for the selected machine IDs.
3. Click one or more blocked applications.
4. Click the **Unblock** button. The window closes.
5. The blocked application no longer displays in the [Application](#) column beside the selected machine IDs.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Application

Filename of the application being blocked.

## Chapter 4

# Agent Procedures

### In This Chapter

Agent Procedures Overview	93
Schedule / Create	94
Distribution	120
Agent Procedure Status	122
Patch Deploy	123
Application Deploy	124
Packager	127
Get File	127
Distribute File	129

**About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Agent Procedures Overview

## Agent Procedures

Use the [Agent Procedures](#) module to create and schedule automated tasks on managed machines.

## Installations

You can schedule the installation of Microsoft and non-Microsoft applications and patches using [Patch Deploy](#) (page 123) and [Application Deploy](#) (page 124).

**Note:** See [Patch Management](#) (page 305) to install Microsoft patches on managed machines.

When a pre-defined install solution cannot be used, use [Packager](#) (page 127) to create a self-extracting file ready for automated distribution.

## File Transfers

Transfer files to and from managed machines using [Get File](#) (page 127) and [Distribute File](#) (page 129).

## Agent Procedure Analysis

You can view the status of all procedures run on a managed machine using [Agent Procedure Status](#) (page 122). You can also spread out the impact agent procedures have on network traffic and server loading using [Distribute](#) (page 120).

## Operating Systems

Customized agent procedures include specifying what type of operating system they should be run on, including managed machines running the Macintosh and Linux.

Functions	Description
<a href="#">Schedule / Create</a> (page 94)	Automates user-defined tasks on managed machines by creating and scheduling agent procedures.
<a href="#">Distribution</a> (page 120)	Minimizes network traffic and server loading by executing agent procedures evenly throughout the day.
<a href="#">Agent Procedure Status</a> (page 122)	Shows the status of agent procedures executed on managed machines: machine ID, group ID, time of the last executed agent procedure, results of the executed agent procedure, and the number of times the agent procedure has been executed.
<a href="#">Patch Deploy</a> (page 123)	Use this wizard tool to create procedures to deploy Microsoft patches to managed machines.
<a href="#">Application Deploy</a> (page 124)	Use this wizard tool to create procedures to deploy non-Microsoft install packages (setup.exe) to managed machines.
<a href="#">Packager</a> (page 127)	An external application that allows users to create customized installation packages deployable on managed machines.
<a href="#">Get File</a> (page 127)	View and manage files uploaded to the KServer from managed machines using the Get File agent procedure command.
<a href="#">Distribute File</a> (page 129)	Write files to all selected managed machines and maintain them.

## Schedule / Create

### Agent Procedures > Schedule / Create

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Schedule / Create** page automates user-defined tasks on managed machines by creating and scheduling agent procedures.

### Folder Trees

Agent procedures are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

#### Always Available

- Manage Files** - See **Manage Files Stored on Server** (page 118) for more information.
- Manage Variables** - See **Variable Manager** (page 117) for more information.
- Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- (Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

#### When a Folder is Selected

- Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

**Note:** See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 119) topic.

- Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- Delete Folder** - Deletes a selected folder.
- Rename Folder** - Renames a selected folder.
- New Procedure** - Opens the **Agent Procedure Editor** (page 96) to create a new procedure in the selected folder of the folder tree.
- Import Folder/Procedure** - Imports a folder or procedure as children to the selected folder in the folder tree.

**Note:** Legacy scripts can be imported into Kaseya 2.

- Export Folder** - Exports the selected folder and all its procedures as an XML file. The XML file can be re-imported.
- Take Ownership - Takes ownership** (page 119) of a folder you do not own. This option only displays for **master role users** (page 600).

#### When a Procedure is Selected

- Edit Procedure** - Opens the **Agent Procedure Editor** (page 96) to edit the selected procedure.
- Delete Procedure** - Deletes the selected procedure.
- Export Procedure** - Exports the selected procedure.
- Rename Procedure** - Renames the selected procedure.

### Creating / Editing Agent Procedures

To create a new procedure, select a cabinet or folder in the middle pane, then click the **New Procedure** button to open the **Agent Procedure Editor** (page 96).

To edit an existing procedure, select the procedure, then click the **Edit Procedure** button to open the

**Agent Procedure Editor** (page 96). You can also double-click a procedure to edit it.

**Note:** Access to creating or editing a procedure depends on your **Folder Rights** (page 119).

## Running / Scheduling / Viewing Agent Procedures

When a procedure is selected in the middle pane, the following tabs display in the right-hand pane:

- **Schedule** - Select one or more machine IDs in this tab's table, then click one of the following action buttons:
  - **Schedule Procedure** - Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:
    - ✓ **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
    - ✓ **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
    - ✓ **Power up if offline** - If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
    - ✓ **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

**Note:** You can stagger the running of scheduled agent procedures using **Agent Procedures > Distribution** (page 120).

- **Run Now** - Run this agent procedure on each selected machine ID immediately.
- **Cancel** - Cancel the scheduled agent procedure on each selected machine ID.
- **View Procedure** - Provides a display only view of the procedure. A user can execute an agent procedure and view it without necessarily being able to edit it. See **Folder Rights** (page 119) for more information.
- **Used by** - Displays a list of other procedures that execute this procedure. Agent procedures that are used by other agent procedures cannot be deleted.

## Agent Procedure Failure Alerts

The **Alerts - Agent Procedure Failure** (page 243) page triggers an alert when an agent procedure fails to execute on a managed machine. For example, if you specify a file name, directory path or registry key in an agent procedure, then run the agent procedure on a machine ID for which these values are invalid, you can be notified about the agent procedure failure using this alerts page.

## Logging Failed Steps in Procedures

The System > **Configure** (page 412) page includes the following option - **Enable logging of procedure errors marked "Continue procedure if step fail"** - If checked, failed steps in procedures are logged. If blank, failed steps in procedures are *not* logged.

## View Definitions

You can filter the display of machine IDs on any agent page using the following agent procedure options in **View Definitions** (page 28).

- **With procedure scheduled/not scheduled**
- **Last execution status success/failed**
- **Procedure has/has not executed in the last N days**

## Agent Procedure Editor

### Creating / Editing Agent Procedures

To create a new procedure, select a cabinet or folder in the middle pane, then click the **New Procedure** button to open the **Agent Procedure Editor** (page 96).

To edit an existing procedure, select the procedure, then click the **Edit Procedure** button to open the **Agent Procedure Editor** (page 96). You can also double-click a procedure to edit it.

**Note:** Access to creating or editing a procedure depends on your **Folder Rights** (page 119).

### The Agent Procedure Editor

The outline of the entire agent procedure displays in the left-hand pane of the editor. The parameters for each statement display in the right-hand pane.

**Note:** See **IF-ELSE-STEP Commands** (page 97) for a detailed explanation of each statement's parameters.

#### Title

- This the first step in the procedure, where you set the name and description of the procedure.

#### Action Buttons

- **New Step** - Creates a step below the currently selected statement.
- **New IF** - Creates a pair of IF-Else statements below the currently selected statement.
- **Toggle Else** - Adds or removes the corresponding Else statement for a selected IF statement. Only displays if an IF statement is selected.
- **Copy** - Copies a single Step or IF statement to the clipboard. Copying an IF statement includes all child statements, so you quickly copy and paste entire IF branches within the same procedure.
- **Paste** - Pastes a Step or IF statement just below a selected statement.
- **Delete** - Deletes the currently selected Step, IF or Else statement.

#### Closing the Editor

- **Save and Close** - Saves and closes the procedure.
- **Save** - Saves the procedure.
- **Save As** - Saves the procedure to a different name.
- **Cancel** - Cancels changes made to the procedure.

#### Drag and Drop

-  - Drag any statement and drop it above another statement.
-  - Drag any statement and drop it below another statement.
-  - Drag any statement and drop it between another statement.
-  - Drag any statement to a procedure Title, IF or Else statement and add it as a child statement.

#### Guidelines

- Click any Step, IF or Else statement in a procedure to see its properties in the right-hand pane. You can edit these properties immediately.
- You can nest steps within multiple IF or Else statements.
- You can toggle the removal of an Else statement without removing its corresponding IF statement.

- You can set a Step to allow a procedure to continue running even if that particular Step fails.

## IF-ELSE-STEP Commands

The following is a summary of standard IF-ELSE-STEP commands used in VSA agent procedures.

<b>IF Definitions</b>	
<b>Application is Running</b> (page 100)	Tests to see if the specified application is running.
<b>Check Registry Value</b> (page 100)	Evaluates the given registry value.
<b>Check 64-bit Registry Value</b> (page 100)	Evaluates the given <b>64-bit</b> (page 114) registry value.
<b>Check Variable</b> (page 101)	Evaluates the given agent variable. See <b>Using Variables</b> (page 115).
<b>Evaluate Expression</b> (page 102)	Compares a variable with a supplied value.
<b>Memory check - Total RAM</b> (page 102)	Evaluates the total amount of memory reported by the latest audit of the agent.
<b>Service is Running</b> (page 102)	Determines if a service is running on the managed machine.
<b>Test File</b> (page 102)	Tests for the existence of a file.
<b>Test File in Directory Path</b> (page 103)	Tests for the existence of a file in the current directory path returned by <b>Get Directory Path From Registry</b> .
<b>Test Registry Key</b> (page 103)	Tests for the existence of the given registry key.
<b>Test 64-bit Registry Key</b> (page 103)	Tests for the existence of the given 64-bit registry key.
<b>True</b> (page 103)	Always returns <code>True</code> , executing <b>IF</b> branch.
<b>User Activity Check</b> (page 103)	Determines whether the user is either: <ul style="list-style-type: none"> <li>• Idle or not logged on, or</li> <li>• Active</li> </ul>
<b>User Is Logged In</b> (page 103)	Tests whether a specific user, or any user, is logged in or not.
<b>User Response is Yes</b> (page 103)	Presents a <b>Yes/No</b> dialog box to the user.
<b>Windows 32 or 64 Bit Check</b> (page 103)	Determines if the current Windows OS is 32 or 64-bit.
<b>STEP Definitions</b>	
<b>Capture Desktop Screenshot</b> (page 104)	Captures a desktop screenshot of the agent machine and uploads it to the Kserver.
<b>Change Domain User Group (Run on Domain Controller)</b> (page 104)	Changes a domain user's membership in a domain user group.
<b>Change Local User Group</b> (page 104)	Changes a local user's membership in a local user group.
<b>Close Application</b> (page 104)	Closes a running application.
<b>Copy File</b> (page 104)	Copies a file from one directory to another.
<b>Copy File – Use Credentials</b> (page 104)	Copies a file from one directory to another using a user credential.
<b>Create Domain User (run on Domain)</b>	Adds a new user to an Active Directory domain

## Agent Procedures

<b>Controller</b> (page 105)	when run on a domain controller.
<b>Create Event Log Entry</b> (page 105)	Creates an event log entry in either the Application, Security or System event log types. You can create a Warning, Error or Informational event with your own description.
<b>Create Local User</b> (page 105)	Adds a new local user account to a machine.
<b>Create Windows File Share</b> (page 105)	Creates a new file share on a Windows machine.
<b>Delete Directory</b> (page 105)	Deletes a directory from the agent machine.
<b>Delete File</b> (page 105)	Deletes a file from the managed machine.
<b>Delete File in Directory Path</b> (page 105)	Deletes file in directory returned by <b>Get Directory Path From Registry</b> .
<b>Delete Registry Key</b> (page 105)	Deletes a key from the registry.
<b>Delete 64-bit Registry Key</b> (page 105)	Deletes a <b>64-bit</b> (page 114) key from the registry.
<b>Delete Registry Value</b> (page 106)	Deletes a value from the registry.
<b>Delete 64-bit Registry Value</b> (page 106)	Deletes a <b>64-bit</b> (page 114) value from the registry.
<b>Delete User</b> (page 106)	Deletes a user from the agent machine.
<b>Disable User</b> (page 106)	Disables a user, preventing logon to the agent machine.
<b>Disable Windows Service</b> (page 106)	Disables a Windows service.
<b>Enable User</b> (page 106)	Enables a previously disabled user, allowing the user to logon to the OS.
<b>Execute File</b> (page 106)	Executes any file as if it was run from the <b>Run</b> item in the <b>Windows</b> Start menu.
<b>Execute File in Directory Path</b> (page 106)	Same as execute file. File location is relative to the directory returned by <b>Get Directory Path From Registry</b> .
<b>Execute Powershell</b> (page 106)	Executes a powershell file, or command with arguments or both.
<b>Execute Procedure</b> (page 107)	Starts another VSA agent procedure on the current machine.
<b>Execute Shell Command</b> (page 107)	Runs any command from a command shell.
<b>Execute Shell Command - Get Results to Variable</b> (page 107)	Executes a shell command and returns output created during and after its execution to a variable.
<b>Execute VBScript</b> (page 107)	Runs a Vbscript, with or without command line arguments.
<b>Get Directory Path From Registry</b> (page 107)	Returns the directory path stored in the registry at the specified location. Result used in subsequent steps.
<b>Get File</b> (page 108)	Gets a file from the managed machine and saves it to the KServer.
<b>Get File in Directory Path</b> (page 108)	Gets a file from the managed machine located relative to the directory returned by <b>Get Directory Path From Registry</b> and saves it to the KServer.
<b>Get URL</b> (page 108)	Returns the text and HTML contents of a URL and stores it to a file on the managed machine.
<b>Get URL (Use Patch File Source Setting)</b> (page 108)	Downloads a file from a given URL to a target folder and file for that agent. Uses the Patch Management > File Source settings.

<b>Get Variable</b> (page 108)	Gets a value from the agent on the managed machine and assigns it to a variable. See <a href="#">Using Variables</a> (page 115).
<b>Get Variable - Random Number</b> (page 108)	Generates a random number.
<b>Get Variable - Universal - Create</b> (page 109)	Gets a variable that persists outside of the immediate procedure's execution.
<b>Get Variable - Universal - Read</b> (page 109)	Reads up to three variables you have previously created using the <a href="#">Get Variable – Universal – Create</a> step.
<b>Give current user admin rights</b> (page 109)	Adds the current user to the local administrator's group on the agent machine, either permanently or for a temporary period of time.
<b>Impersonate User</b> (page 109)	Specifies the user account to use when executing a file or shell when <a href="#">Execute as the logged on user</a> is specified in a subsequent command.
<b>Install Apt-Get Package (Linux)</b> (page 109)	Silently installs a package using the <code>apt-get</code> command in Linux.
<b>Install Deb Package (Linux)</b> (page 109)	Silently installs a Debian package on any Linux OS that supports <code>.deb</code> packages.
<b>Install DMG (OS X)</b> (page 109)	Silently installs a <code>.DMG</code> package in OS X.
<b>Install MSI</b> (page 110)	Installs an MSI file for Windows.
<b>Install PKG (OS X)</b> (page 110)	Silently installs a <code>.PKG</code> package in OS X.
<b>Install RPM (Linux)</b> (page 110)	Silently installs an RPM package on any Linux OS that supports installing RPMs.
<b>Log off Current User</b> (page 110)	Automatically logs off the current user.
<b>Pause Procedure</b> (page 110)	Pauses the procedure for N seconds.
<b>Reboot</b> (page 110)	Reboots the managed machine.
<b>Reboot with warning message</b> (page 110)	Reboots a machine, displaying a warning message to the end-user before the reboot process occurs.
<b>Remove Windows File Share</b> (page 110)	Removes a file share from a Windows agent.
<b>Rename Locked File</b> (page 110)	Renames a file that is currently in use.
<b>Rename Locked File in Directory Path</b> (page 110)	Renames a file currently in use in directory returned by <a href="#">Get Directory Path From Registry</a> .
<b>Schedule Procedure</b> (page 111)	Schedules an agent procedure to run on a specified machine.
<b>Send Email</b> (page 111)	Sends an email to one or more recipients.
<b>Send Message</b> (page 111)	Displays a message in a dialog box on the managed machine.
<b>Send URL</b> (page 111)	Opens a browser to the specified URL on the managed machine.
<b>Set Registry Value</b> (page 111)	Sets the registry value to a specific value.
<b>Set 64-bit Registry Value</b> (page 111)	Sets the <a href="#">64-bit</a> (page 114) registry value to a specific value.
<b>Start Windows Service</b> (page 112)	Runs a Start command for a Windows service, if it exists.
<b>Stop Windows Service</b> (page 112)	Runs a Start command for a Windows service if it

## Agent Procedures

	exists.
<b>Transfer File</b> (page 112)	Transfers a file from the agent machine running this step to another agent machine.
<b>Uninstall by Product GUID</b> (page 112)	Silently uninstalls a product based on its MSI GUID.
<b>Unzip file</b> (page 112)	Extracts the contents of a specified zip file to a target folder.
<b>Update System Info</b> (page 112)	Updates the selected <b>System Info</b> field with the specified value.
<b>Use Credential</b> (page 113)	Specifies that <b>Set Credential</b> should be used when <b>Execute as the logged on user</b> is specified in a subsequent command.
<b>Windows Service Recovery Settings</b> (page 113)	Sets the Service Recovery Settings for any given service in Windows.
<b>Write Directory</b> (page 113)	Writes a directory from the server to the managed machine.
<b>Write File</b> (page 113)	Writes a file stored on the KServer to the managed machine.
<b>Write File - From Agent</b> (page 113)	Transfers a file from another agent machine to the agent machine running this step.
<b>Write File in Directory Path</b> (page 113)	Writes a file stored on the KServer to the managed machine using the directory returned by <b>Get Directory Path From Registry</b> .
<b>Write Procedure Log Entry</b> (page 114)	Writes a string to the Agent Procedure Log.
<b>Write text to file</b> (page 114)	Writes text to a file on the agent machine.
<b>Zip Directory</b> (page 114)	Compresses a directory and any subdirectories or files it contains into a zip file on the agent machine.
<b>Zip File(s)</b> (page 114)	Compresses a single file or files into a zip file on the agent machine.

## IF Commands

### Application is Running

Checks to see if a specified application is currently running on the managed machine. If the application is running, the **IF** command is executed; otherwise, the **ELSE** command is executed. When this option is selected from the drop-down list, the **Enter the application name** field appears. Specify the process name for the application you want to test. For example, to test the `Calculator` application, specify `calc.exe`, which is the process name that displays in the **Processes** tab of the Windows **Task Manager**.

### Check Registry Value / Check 64-Bit (page 114) Registry Value

After entering the registry path, the value contained in the key is returned. A check can be made for existence, absence, equality, or size differences. For example, `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\AppPaths\AgentMon.exe\path` contains the directory path identifying where the agent is installed on the target machine. The test determines if the value stored for this key exists, thereby verifying the agent is installed.

A backslash character \ at the end of the key returns the default value of that key. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WORDPAD.EXE\ returns a default value, such as %ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE

The available tests are:

- `Exists` : true if the registry key exists in the hive.
- `Does Not Exist` : true if the registry key does *not* exist in the hive.
- `=` : true if value of the registry key equals the test value.
- `Not =` : true if value of the registry key does *not* equal the test value.
- `>` : true if value of the registry key is greater than the test value (value must be a number).
- `>=` : true if value of the registry key is greater than or equal to the test value (value must be a number).
- `<` : true if value of the registry key is less than the test value (value must be a number).
- `<=` : true if value of the registry key is less than or equal to the test value (value must be a number).
- `Contains` : true if the test value is a sub string of the registry key value (value must be a string).
- `Not Contains` : true if the test value is *not* a sub string of the registry key value (value must be a string).

## Check Variable

Enter a variable name, in the form #var\_name#, in the space provided. **Check Variable** evaluates the current values assigned #var\_name# and compares it with the supplied value. The supplied value may also be another variable name in the form of #var\_name2#. If the check is true, **IF** commands are executed. If the check is false, **ELSE** steps are executed. See **Using Variables** (page 115). The available tests are:

- `Exists` : true if the variable exists.
- `Does Not Exist` : true if the variable does *not* exist.
- `=` : true if value of the variable equals the test value.
- `Not =` : true if value of the variable does *not* equal the test value.
- `>` : true if value of the variable is greater than the test value.
- `>=` : true if value of the variable is greater than or equal to the test value.
- `<` : true if value of the variable is less than the test value.
- `<=` : true if value of the variable is less than or equal to the test value.
- `Contains` : true if the test value is a sub string of the variable value.
- `Not Contains` : true if the test value is *not* a sub string of the variable value.
- `Begins With` : true if the test value begins with the variable value.
- `Ends With` : true if the test value ends with the variable value.

For the tests `=`, `Not =`, `>`, `>=`, `<`, and `<=` the variables compared may be a string, a number, a date in the format of `yyyy/mm/dd` or `yyyy/mm/dd hh:mm` or `yyyy/mm/dd hh:mm:ss`, or a version number containing dots or commas such as `1.2.3` or `4,5,6,7`. If a date format is specified, it may be offset using `+ dd:hh:mm:ss` or `- dd:hh:mm:ss`. Only `dd` days are required; `hh` hours, `mm` minutes, and `ss` seconds may be omitted and are assumed to be zero when absent. `CURRENT_TIMESTAMP` may be specified to indicate that the current time be substituted in the comparison at the time the procedure is executed. e.g. `CURRENT_TIMESTAMP - 7:12:00:00` will be evaluated as 7 days and 12 hours subtracted from the time that the procedure is executed.

### Evaluate Expression

Enter an expression containing one or more variable names, in the form `#var_name#`, in the space provided. **Evaluate Expression** uses the current value assigned to each `#var_name#`, evaluates the mathematical expression, and compares it with the supplied value. The supplied value may also be another expression. The mathematical expression may contain `+`, `-`, `*`, `/`, `(`, and `)`. e.g. `(3.7 + (200 * #countA#)) / (#countB# - #countC#)`. If the check is true, **IF** steps are executed. If the check is false, **ELSE** steps are executed. The available tests are:

- `=` : true if value of the variable equals the test value.
- `Not =` : true if value of the variable does not equal the test value.
- `>` : true if value of the variable is greater than the test value.
- `>=` : true if value of the variable is greater than or equal to the test value.
- `<` : true if value of the variable is less than the test value.
- `<=` : true if value of the variable is less than or equal to the test value.

**Note:** Cannot be used with `Exists`, `Does Not Exist`, `Contains`, or `Not Contains` operators.

### Memory check - Total RAM

Evaluates the total amount of memory reported by the latest audit of the agent. This could come in helpful in ensuring a system meets the resource requirements of an application before an installation is attempted.

Operating systems supported: Windows, OS X, Linux

### Service is Running

Determines if a service is running on the managed machine. Specify the *service name*.

- True if the service name is running.
- False if the service name is stopped or does not exist.

**Note:** Be sure to use the *service name* of the service, not the *display name* of the service. For example, the *display name* of the service for Microsoft SQL Server is `SQL Server (MSSQLSERVER)`, but the *service name* of the service is `MSSQLSERVER`. For Windows machines, right click any service in the Services window and click the Properties option to see the *service name* of that service.

### Test File

Determines if a file exists on a managed machine. Enter the full path and file name. **Test File** compares the full path and file name with the supplied value. If the check is true, **IF** commands are executed. If the check is false, **ELSE** steps are executed.

**Note:** Environment variables such as `%windir%\notepad.exe` are acceptable.

The available tests are:

- `Exists` : true if the full path and file name exists.
- `Does not Exist` : true if the full path and file name does *not* exist.
- `Contains` : true if the test value is a sub string of the file content.
- `Not Contains` : true if the test value is *not* a sub string of the file content.
- `Begins With` : true if the test value begins with the variable value.
- `Ends With` : true if the test value ends with the variable value.

## Test File in Directory Path

Tests the specified file located at the path returned using the [Get Directory Path From Registry](#) step. The available tests are:

- `Exists` : true if the file name exists.
- `Does not Exist` : true if the file name does *not* exist.
- `Contains` : true if the test value is a sub string of the file content.
- `Not Contains` : true if the test value is *not* a sub string of the file content.
- `Begins With` : true if the test value begins with the variable value.
- `Ends With` : true if the test value ends with the variable value.

## Test Registry Key / Test 64-bit (page 114) Register Key

Tests for the existence of a registry key. [Test Registry Key](#) differs from [Check Registry Value](#) since it can check for a directory level registry entry that only contains more registry keys (no values).

## True

Selecting `True` directs the **IF** commands to execute. Use `True` to directly execute a series of steps that do not require any decision points, such as determining whether a file exists using [Test File](#).

## User Activity Check

Determines whether the user is either:

- Idle or not logged on, or
- Active

Operating systems supported: Windows, OS X, Linux

## User Is Logged In

Tests to see if a specific user or any user is logged on the managed machine. Enter the machine user's logon name or leave the field blank to check for any user logged on. The **IF** commands are executed if a user is logged on. The **ELSE** steps are executed if the user is not logged on.

## User Response is Yes

Displays a dialog box on the managed machine with **Yes** and **No** buttons. Also carries out the **ELSE** command if a specified amount of time has timed out. If **Yes** is selected by the machine user, the **IF** command is executed. If the selection times out or the machine user selects **No**, the **ELSE** command is executed. This function requests the machine user's permission to proceed with the agent procedure. This query is useful for agent procedures that require a reboot of the managed machine before completion.

Procedure variables, for example `#varName#`, may be used inside **User Response is Yes** fields to dynamically generate messages based on procedure data.

## Windows 32 or 64 Bit Check

Determines if the current Windows OS is 32 or 64-bit.

Operating systems supported: Windows

## STEP Commands

### Capture Desktop Screenshot

Captures a desktop screenshot of the agent machine and uploads it to the Kserver. The screenshot is saved as a PNG file with a unique name in a folder dedicated to that agent. You can access these files from the Agent > [Documents](#) (page 143) page or from [Live Connect](#) (page 380). End-user notification options must be selected based on the level of user notification desired, silently capturing a screenshot, notifying the user that the capture will take place, or asking to approve the capture. A custom message can be entered if end-user notification or permission requesting is selected. Otherwise a standard message displays.

Operating systems supported: Windows, OS X

### Change Domain User Group (Run on Domain Controller)

Changes a domain user's membership in a domain user group. This [STEP](#) must be run on a domain controller. Enter the domain username of the member being added or removed from the domain user group. Then select whether to add or remove membership. Then select the domain user group.

Operating systems supported: Windows

### Change Local User Group

Changes a local user's membership in a local user group. Enter the local username of the member being added or removed from the local user group. Then select whether to add or remove membership. Then select the group.

Operating systems supported: Windows

### Close Application

If the specified application is running on the managed machine, then that application is closed down. Specify the process name for the application you want to close. For example, to close the Calculator application, specify `calc.exe`, which is the process name that displays in the [Processes](#) tab of the Windows [Task Manager](#).

### Copy File

Copies a file from one directory to another on the agent machine. If the target file exists, you must check a box to overwrite an existing file. Be sure to keep in mind folder syntax when running this [STEP](#) across different operating systems, for example, `c:\temp\tempfile.txt` for Windows and `/tmp/tempfile.txt` for OS X and Linux.

Operating systems supported: Windows, OS X, Linux

### Copy File – Use Credentials

Copies a file from a directory on a machine and attempts to copy the file to a target directory and filename. The copy process uses either:

- The user credential specified for an agent using Agent > [Set Credentials](#) (page 83), or
- The user credential specified by an [Impersonate User](#) step before this step.

This [STEP](#) is mostly used for accessing files across network UNC shares. If the target file exists, you must check a box to overwrite an existing file. Be sure to keep in mind folder syntax when running this [STEP](#) across different operating systems, for example, `c:\temp\tempfile.txt` for Windows and `/tmp/tempfile.txt` for OS X and Linux.

Operating systems supported: Windows, OS X, Linux

### Create Domain User (run on Domain Controller)

Adds a new user to an Active Directory domain when run on a domain controller. Enter a domain user name to create, then a password that meets the domain's complexity requirements for user accounts, then select the domain group the user will be added to, either `Domain Users` or `Domain Admins`.

Operating systems supported: Windows

### Create Event Log Entry

Creates an event log entry in either the Application, Security or System event log types. You can create a Warning, Error or Informational event with your own description. The created event is hard-coded to use an Event ID of 607.

Operating systems supported: Windows

### Create Local User

Adds a new local user account to a machine. Enter a local user name to create, then a password that meets local user account complexity requirements, then select the group the user will be added to.

Operating systems supported: Windows, OS X, Linux

### Create Windows File Share

Creates a new file share on a Windows machine. You must type in the name of the file share as it will be accessed over the network, and enter the source folder on the agent for the file share. This folder will be created if it does not yet exist.

Operating systems supported: Windows

### Delete Directory

Deletes a directory from an agent machine. Ensure you have your directory syntax correct for Windows vs. OS X/ Linux. To ensure all sub-directories and files are also removed, check the [Recursively delete subdirectories and files](#) checkbox.

Operating systems supported: Windows, OS X, Linux

### Delete File

Deletes a file on a managed machine. Enter the full path and filename.

**Note:** Environment variables are acceptable if they are set on a user's machine. For example, using a path `%windir%\notepad.exe` would be similar to `C:\windows\notepad.exe`.

**Note:** You can delete a file that is currently in use using the [Rename Locked File](#) command.

### Delete File in Directory Path

Deletes the specified file located at the path returned using the [Get Directory Path From Registry](#) command.

### Delete Registry Key / Delete 64-bit (page 114) Registry Key

Deletes the specified registry key and all its sub-keys.

### Delete Registry Value / Delete 64-bit (page 114) Registry Value

Deletes the value stored at the specified registry key.

### Delete User

Deletes a user from the agent machine.

Operating systems supported: Windows, OS X, Linux

### Disable User

Disables a user, preventing logon to the agent machine.

Operating systems supported: Windows, OS X, Linux

### Disable Windows Service

Disables a Windows service.

Operating systems supported: Windows

### Enable User

Enables a previously disabled user, allowing the user to logon to the OS.

Operating systems supported: Windows, OS X

### Execute File

Executes the specified file on the managed machine. This function replicates launching an application using the **Run...** command located in the Microsoft Windows **Start** menu. This function takes three parameters:

- Full path filename to the .exe file.
- Argument list to pass to the .exe file
- Option for the procedure to wait until the .exe completes or not.

**Note:** Environment variables are acceptable, if they are set on a user's machine. For example, using a path %windir%\notepad.exe, would be similar to C:\windows\notepad.exe.

If **Execute as the logged on user** is selected, then a credential must be specified by running either the **Impersonate User** (page 109) or **Use Credential** (page 113) command before this command. If run **Execute as the system account** is selected, execution is restricted to the agent's system level access.

### Execute File in Directory Path

Same as **Execute File** except the location of the .exe file is located at the path returned from a **Get Directory Path From Registry** command.

If **Execute as the logged on user** is selected, then a credential must be specified by running either the **Impersonate User** (page 109) or **Use Credential** (page 113) command before this command. If run **Execute as the system account** is selected, execution is restricted to the agent's system level access.

### Execute Powershell

Executes a powershell script, including:

- a Powershell .PS1 file
- a Powershell command with special arguments
- a combination of both

Operating systems supported: Windows XP SP3+/Server 2008 with Powershell add-on, Windows 7, Windows Server 2008

### Execute Procedure

Causes another named procedure to execute. Use this capability to string multiple **IF-ELSE-STEP** procedures together. If the procedure no longer exists on the KServer, an error message displays next to the procedure drop-down list. You can use this command to run a **system procedure** (page 599). You can nest procedures to 10 levels.

### Execute Shell Command

Allows the procedure to pass commands to the command interpreter on the managed machine. When this command is selected, the field **Enter the command to execute in a command shell** is displayed. Enter a command in the field. The command must be syntactically correct and executable with the OS version on the managed machine. *Commands and parameters containing spaces should be surrounded by quotes*. Since the command is executed relative to the agent directory, absolute paths should be used when entering commands.

**Note:** Execute Shell Command opens a command prompt window on the managed machine to execute in. If you do not want a window opening on the managed machine, because it might confuse users, put all the commands in a batch file. Send that file to the managed machine using the **Write File** command. Then run the batch file with the **Execute File** command. **Execute File** does not open a window on the managed machine.

If **Execute as the logged on user** is selected, then a credential must be specified by running either the **Impersonate User** (page 109) or **Use Credential** (page 113) command before this command. If run **Execute as the system account** is selected, execution is restricted to the agent's system level access.

### Execute Shell Command - Get Results to Variable

Executes a shell command and returns output created during and after its execution to a variable. The variable must be referred to in subsequent steps as #global:cmdresults#.

Operating systems supported: Windows, Linux, OS X

### Execute VBScript

Runs a Vbscript, with or without command line arguments. If the Vbscript displays a popup window or notifies the end user, check the box for **Use Wscript instead of Cscript**.

Operating systems supported: Windows

### Get Directory Path From Registry

Returns a file path stored in the specified registry key. Use this command to fetch the file location. For instance, use this command to find the directory where an application has been installed. The result can be used in subsequent steps by:

- **Delete File in Directory Path**
- **Execute File in Directory Path**
- **Get File in Directory Path**
- **Rename Locked File in Directory Path**

## Agent Procedures

- [Test File in Directory Path](#) (an IF command)
- [Write File in Directory Path](#)

### Get File

Upload the file at the specified path from the managed machine. Be sure to enter a full path filename that you want to upload. Example: `news\info.txt`. Folders are created when the [Get File](#) command is run, if they don't already exist. The file is stored on the KServer in a private directory for each managed machine. View or run the uploaded file using Agent Procedures > [Get File](#) (page 127).

- Optionally, existing copies of uploaded files are renamed with a `.bak` extension prior to the next upload of the file. This allows you to examine both the latest version of the file and the previous version.
- Optionally create a [Get File](#) alert if the uploaded file *differs* or is the *same* from the file that was uploaded previously. *You must create a Get File alert for a machine ID* using the Monitor > [Alerts - Get File](#) (page 227) page to enable the sending of an alert using the [Get File](#) command. Once defined for a machine ID, the same [Get File](#) alert is *active for any agent procedure* that uses a [Get File](#) command and is run on that machine ID. Turn off alerts for specific files in the agent procedure editor by selecting one of the without alerts options.

### Get File in Directory Path

Just like the [Get File](#) command but it adds the path returned from the [Get Directory Path From Registry](#) command to the beginning of the remote file path. Access the uploaded file using the Agent Procedures > [Get File](#) (page 127) function.

### Get URL

Returns the text and HTML contents of a URL and stores it to a file on the managed machine. To demonstrate this to yourself, try specifying `www.kaseya.com` as the URL and `c:\temp\test.htm` as the file to store the contents of this URL. A copy of the web page is created on the managed machine that contains all of the text and HTML content of this webpage. You can search the contents of the file on the managed machine in a subsequent command.

Another use is to download an executable file that is available from a web server, so that you don't need to upload the file to the VSA server nor use the VSA's bandwidth to write the file down to each agent. You can use a subsequent command to run the downloaded executable on the managed machine.

### Get URL (Use Patch File Source Setting)

Downloads a file from a given URL to a target folder and file for that agent. Uses the Patch Management > [File Source](#) (page 340) settings.

Operating systems supported: Windows

### Get Variable

Defines a new agent variable. When the procedure step executes, the system defines a new variable and assigns it a value based on data fetched from the managed machine's agent.

**Note:** See [Using Variables](#) (page 115) for the types of variable values supported by the [Get Variable](#) command.

### Get Variable - Random Number

Generates a random number which can then be accessed as the variable `#global:rand#` in a subsequent step.

Operating systems supported: Windows, OS X, Linux

### **Get Variable - Universal - Create**

Gets a variable that persists outside of the immediate procedure's execution. This can be useful for passing a variable to another agent procedure using the [Schedule Procedure](#) step. You can create up to three variables. You can enter either string data or variables created in an earlier step. Variables created using this step can only be read using the [Get Variable – Universal – Read](#) step in any subsequent step.

Operating systems supported: Windows, OS X, Linux

### **Get Variable - Universal - Read**

Reads up to three variables you have previously created using the [Get Variable – Universal – Create](#) step. These variables must be referred to as #global:universal1#, #global:universal2#, and #global:universal3#. Please see the initial [Get Variable – Universal – Create](#) step for more detail.

Operating systems supported: Windows, OS X, Linux

### **Give current user admin rights**

Adds the current user to the local administrator's group on the agent machine, either permanently or for a temporary period of time. This change does *not* take effect until the user logs off. It is recommended you leverage the [Log off Current User](#) step.

Operating systems supported: Windows

### **Impersonate User**

Enter a username, password, and domain for the agent to logon with. This command is used in a procedure before an [Execute File](#), [Execute File in Directory Path](#) or [Execute Shell Command](#) that specifies the [Execute as the logged on user](#) option. Leave the domain blank to log into an account on the local machine. Use [Impersonate User](#) to run an agent procedure using a credential specified *by agent procedure*. Use [Use Credential](#) to run an agent procedure using a credential specified *by managed machine*.

### **Install Apt-Get Package (Linux)**

Silently installs a package using the `apt-get` command in Linux.

Operating systems supported: Linux

### **Install Deb Package (Linux)**

Silently installs a Debian package on any Linux OS that supports `.deb` packages.

Operating systems supported: Linux

### **Install DMG (OS X)**

Silently installs a `.DMG` package in OS X. If the package is formatted as an `Application`, it is copied to the `/Applications` folder. If the `.DMG` contains a `.PKG` installer within it, Kaseya attempts to install it.

Operating systems supported: OS X

## Agent Procedures

### Install MSI

Installs an MSI file for Windows. Options can be selected to either run a quiet installation or to avoid automatically restarting the computer after installation if it is requested.

Operating systems supported: Windows

### Install PKG (OS X)

Silently installs a .PKG package in OS X.

Operating systems supported: OS X

### Install RPM (Linux)

Silently installs an RPM package on any Linux OS that supports installing RPMs.

Operating systems supported: Linux

### Log off Current User

Automatically logs off the current user. An optional warning that the log-off process is about to begin can be entered and displayed to the end-user.

Operating systems supported: Windows, OS X

### Pause Procedure

Pause the procedure for N seconds. Use this command to give Windows time to complete an asynchronous task, like starting or stopping a service.

### Reboot

Unconditionally reboots the managed machine. To warn the user first, use the [User Response is Yes](#) command before this command. A [User Response is Yes](#) command prompts the user before rebooting their machine.

### Reboot with warning message

Reboots a machine, displaying a warning message to the end-user before the reboot process occurs.

Operating systems supported: Windows, OS X

### Remove Windows File Share

Removes a file share from a Windows agent.

Operating systems supported: Windows

### Rename Locked File

Renames a file that is currently in use. The file is renamed the next time the system is rebooted. The specified filename is a complete file path name. Can be used to delete a file that is currently in use if the "new file name" is left blank. The file is deleted when the system is rebooted.

### Rename Locked File in Directory Path

Renames a file that is currently in use that is located in the path returned from a [Get Directory Path From Registry](#) command. The file is renamed the next time the system is rebooted. Can be used to delete a

file that is currently in use if the "new file name" is left blank. The file is deleted when the system is rebooted.

### Schedule Procedure

Schedules a procedure to run on a specified machine. Optionally specifies the time to wait after executing this step before running the procedure and the specified machine ID to run the procedure on. If no machine is specified, then the procedure is run on the same machine running the agent procedure. Enter the complete name of the machine, for example, `machine.unnamed.org`. *This command allows an agent procedure running on one machine to schedule the running of an agent procedure on a second machine.* You can use this command to run a **system** (page 599) procedure. You can nest procedures to 10 levels.

### Send Email

Sends an email to one or more recipients. Specifies the subject and body text of the email.

### Send Message

Sends the entered message to a managed machine. An additional checkbox, if checked, sends the message immediately. If unchecked, sends the message after the user clicks the flashing agent system tray icon.

### Send URL

Displays the entered URL in a web browser window on the managed machine. An additional checkbox, if checked, displays the URL immediately. If unchecked, the URL is displayed after the user clicks the flashing agent system tray icon.

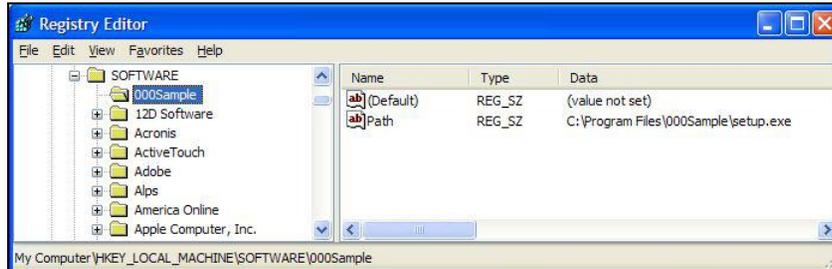
### Set Registry Value / Set 64-bit (page 114) Registry Value

Writes data to the specified registry value. This function takes three parameters:

- **Enter the full path to a registry key containing a value** - Specify the (Default) value for a registry key by adding a trailing backslash \. Otherwise specify a name for an existing value or to create a new value. See Name column in image below.  
Example of setting the (Default) value: `HKEY_LOCAL_MACHINE\SOFTWARE\000Sample\`
- **Enter the data to write to the registry value**
- **Select the data type**
  - `REG_SZ` - String value.
  - `REG_BINARY` - Binary data displayed in hexadecimal format.
  - `DWORD` - Binary data limited to 32 bits. Can be entered in hexadecimal or decimal format.
  - `REG_EXPAND_SZ` - An "expandable" string value holding a variable. Example: `%SystemRoot%`.

## Agent Procedures

- REG\_MULTI\_SZ - A multiple string array. Used for entering more than one value, each one separated by a \0 string. Use \\0 to include \0 within a string array value.



### Start Windows Service

Runs a Start command for a Windows service, if it exists.

Operating systems supported: Windows

### Stop Windows Service

Runs a Start command for a Windows service if it exists.

Operating systems supported: Windows

### Transfer File

Transfers a file from the agent machine running this step to another agent machine. Enter the fully qualified machine ID of the *target machine*, for example, *mymachine.root.kaseya*. Then enter the full path and file name of the source file you wish to send *from the currently selected agent*. Then enter the full path and file name of the target file on the target machine.

Operating systems supported: Windows

### Uninstall by Product GUID

Silently uninstalls a product based on its MSI GUID.

Operating systems supported: Windows

### Unzip file

Extracts the contents of a specified zip file to a target folder, with an option to automatically overwrite any previously existing target files or folders.

Operating systems supported: Windows, OS X, Linux

### Update System Info

Updates the selected **System Info** field with the specified value for the machine ID this procedure runs on. The **System Info** fields you can update include all columns in **vSystemInfo** (page 506) except **agentGuid**, **emailAddr**, **Machine\_GroupID**, **machName**, and **groupName**. **vSystemInfo** column information is used by Audit > **System Info** (page 140), Agent > **System Status** (page 31), the **Filter Aggregate Table** (page 30) in **View Definitions**, and the **Aggregate Table** (page 153) report. You can update a **System Info** field using any string value, including the value of any previously defined agent procedure variable.

## Use Credential

Uses the credentials set for the machine ID in **Set Credential** (page 83). This command is used in a procedure before an **Execute File**, **Execute File in Directory Path** or **Execute Shell Command** that specifies the **Execute as the logged on user** option. Also used to access a network resource requiring a credential from a machine when a user is not logged on. Use **Impersonate User** to run an agent procedure using a credential specified *by agent procedure*. Use **Use Credential** to run an agent procedure using a credential specified *by managed machine*.

**Note:** A procedure execution error is logged if a **Set Credential** procedure command encounters an empty username.

**Note:** Patch Management > Patch Alert (page 342) can alert you—or run an agent procedure—if a machine ID's credential is missing or invalid.

## Windows Service Recovery Settings

Sets the Service Recovery Settings for any given service in Windows. Specify the name of the service you wish to modify, then set both the first and second restart failure options and any subsequent restart failure options.

Operating systems supported: Windows

## Write Directory

Writes a selected directory, including subdirectories and files, from **Manage Files Stored on Server** (page 118) to the full path directory name specified on the managed machine.

## Write File

Writes a file selected from **Manage Files Stored on Server** (page 118) to the full path filename specified on the managed machine. Enter a new filename if you want the file to be renamed.

Each time a procedure executes the **Write File** command, the agent checks to see if the file is already there or not by hashing the file to verify integrity. If not, the file is written. If the file is already there, the procedure moves to the next step. You can repeatedly run a procedure with **Write File** that sends a large file to a managed machine and know that the VSA only downloads that file once.

**Note:** Environment variables are acceptable if they are set on a user's machine. For example, using the path `%windir%\notepad.exe` would be equivalent to `C:\windows\notepad.exe`.

## Write File - From Agent

Transfers a file from another agent machine to the agent machine running this step. Transfers a file between agents. Similar to the previous **Transfer File** step, though in this case you enter the fully qualified machine ID of the *source machine* that has the file you wish to send *to the currently selected agent*. First enter the full path and file name of the file you wish to send from the source machine. You then enter the full path and the file name to be created on the target machine.

Operating systems supported: Windows

## Write File in Directory Path

Writes the specified filename to the path returned from a **Get Directory Path From Registry** command.

## Agent Procedures

### Write Procedure Log Entry

Writes the supplied string to the Agent Procedure Log for the machine ID executing this agent procedure.

### Write text to file

Writes text to a file on the agent machine, either by appending text to an existing file or by creating a new file if none exists. You enter the text to write to the file, then enter the full path and file name on the agent machine the text will be written to. You can optionally overwrite the entire file with the text you have entered if the file already exists.

Operating systems supported: Windows, OS X, Linux

### Zip Directory

Compresses a directory and any subdirectories or files it contains into a zip file on the agent machine. Enter the full path to be compressed, which can contain wildcards. Then enter the full path and file name of the zip file to be created or updated. If the target zip file already exists, optionally check a box to overwrite it.

Operating systems supported: Windows, OS X, Linux

### Zip File(s)

Compresses a single file or files into a zip file on the agent machine. Enter the full path of the file or files to be compressed. Then enter the full path and filename of the zip file to be created or updated. If the target zip already exists, optionally check a box to overwrite it.

Operating systems supported: Windows, OS X, Linux

## 64-Bit Commands

### Accessing 64-bit Registry Values

Five 64-bit registry commands and one 64-bit parameter are available in agent procedures. 64-bit Windows isolates registry usage by 32-bit applications by providing a separate logical view of the registry. The redirection to the separate logical view is enabled automatically and is transparent for the following registry keys:

- HKEY\_LOCAL\_MACHINE\SOFTWARE
- HKEY\_USERS\\*\SOFTWARE\Classes
- HKEY\_USERS\\*\_Classes

Since the Kaseya agent is a 32-bit application, you must use the following commands and parameter to access the registry data that are stored in the above keys by the 64-bit applications.

#### *IF Commands*

- Check 64-bit Registry Value
- Test 64-bit Registry Key

#### *STEP Commands*

- Delete 64-bit Registry Value
- Delete 64-bit Registry Key
- Set 64-bit Registry Value
- 64-bit Registry Value parameter in the Get Variable command

## Specifying 64-bit Paths in File Commands

The following commands...

- [Delete File](#)
- [Write File](#)
- [Execute File](#)
- [Rename Locked File](#)
- [Get File](#)

... can specify 64-bit directories using the following variables:

Use This Environment Variable	To Target This Directory
%windir%\sysnative	<drive>:\Windows\System32
%ProgramW6432%	<drive>:\Program Files
%CommonProgramW6432%	<drive>:\Program Files\Common Files

For compatibility reasons, Microsoft has placed 64-bit system files in the `\Windows\system32` directory and 32-bit system files in the `\Windows\SysWOW64` directory. Similarly, 64-bit application files are installed to the `\Program Files` and 32-bit application files are installed to the `\Program Files (x86)` folder. Since the Kaseya agent is a 32-bit application, when a file path containing `\Windows\system32` or `\Program Files` is specified on a 64-bit machine, the file access is automatically redirected to the `\Windows\SysWOW64` or `\Program Files (x86)` folders. To access files in `\Windows\system32` and `\Program Files` folders, use these environment variables when specifying parameters for these file commands.

## In Directory Path Commands

The [Get Directory Path From Registry](#) command—and any subsequent [...In Directory Path](#) command—cannot be used to access files in the `\Program Files` and `\Windows\System32` directories on a target 64-bit machine. These commands can still access 32-bit or 64-bit files in any other folder.

## Identifying 64-bit Machines

64-bit machine IDs typically display a `x64` in the [Version](#) column of audit pages.

## Using Variables

Use variables to store values that can be referenced in multiple procedure steps. Variables are passed automatically to nested procedures.

- **Three Methods for Creating Variables:**
  - **Procedure Variables** - Use the [Get Variable](#) command within a procedure to create a new variable name without any special characters. Example: `VariableName`. In subsequent steps, including steps in nested procedures, reference the variable by bracketing the variable name with the `#` character. Example: `#VariableName#`.

*Note: Procedures variables cannot be referenced outside of the procedure or nested procedures that use them except for GLOBAL variables. A procedure variable is only visible to the section of the procedure it was created in and any child procedures. Once a procedure leaves the THEN clause or ELSE clause the variable was created in, the variable is out of scope and no longer valid. Use GLOBAL Variables, described below, to maintain visibility of a variable after leaving the THEN clause or ELSE clause the variable was created in.*

- **Managed Variables** - Use the [Variable Manager](#) (page 117) to define variables that can be used repeatedly in different procedures. You can maintain multiple values for each managed variable, with each value applied to one or more group IDs. Managed variables cannot be re-assigned new values within a procedure. Within a procedure, reference a managed

variable by bracketing the variable name with the < and > character. Example:  
<VariableName>.

- **GLOBAL Variables** - Non-GLOBAL variables cannot return a changed value of a procedure variable defined by its parent procedure. Non-GLOBAL variables initialized in the child procedure also cannot be passed back to the parent. Variables named with the prefix **GLOBAL:** (case-insensitive followed by a colon) can pass changed values from the child to the parent, whether the variable is initialized in the parent or the child procedure. Subsequent child procedures can make use of any GLOBAL variable initialized in any earlier step, regardless of whether that global variable is initialized in a parent procedure or another child procedure.
- **Where Used** - Once variables are created you can include them, in their bracketed format, *in any text entry field* displayed by an IF-ELSE-STEP dialog box.
- **Case Sensitivity** - Variable names are case sensitive.
- **Reserved Characters** - Because the <, > and # characters are used to identify variable names, these characters must be entered *twice* as regular text in a command line. For example the following command `c:\dir >> filelist.txt` is interpreted at procedure runtime as `c:\dir > filelist.txt`.
- **Types of Variable Values Possible** - The following are the types of variable values typically obtained by using the **Get Variable** parameter.
  - **Registry Value** - Data from the specified registry value on the managed machine.
  - **File Content** - Data from a specified file on the managed machine.
  - **Constant Value** - Specified constant as typed in the procedure editor.
  - **Agent Install Directory Path** - Directory in which the agent is installed on the managed machine.
  - **Agent Install Drive** - Drive in which the agent is installed on the managed machine, such as `c:\`.
  - **Agent Working Directory Path** - Working directory on the managed machine as specified using **Agent > Working Directory** (page 78).

**Warning: Do not delete files and folders in the working directory. The agent uses the data stored in the working directory to perform various tasks.**

- **User Temporary Directory Path** - The temporary directory for the user currently logged on the managed machine. This path is the expansion of the `%TEMP%` environment variable for the currently logged on user. If no user is logged on, it is the default Windows temporary directory.
- **Machine.Group ID** - Machine ID of the agent executing the procedure.
- **File Version Number** - The software version number of the specified file on the managed machine. For example, an `exe` or `dll` file often contain the version number of their release.
- **File Size** - Size in bytes of the specified file on the managed machine.
- **File Last Modified Date** - The last modified date and time in universal time, coordinated (UTC) of the specified file on the managed machine in the format of `yyyy/mm/dd hh:mm:ss`.
- **Automatic SQL View Data Variables** - SQL view parameters are available as automatically declared procedure variables. Automatic variables enable you to skip using the **GetVariable** command before making use of the variable in a step. Use the format `#SqlViewName.ColumnName#` in a procedure to return the value of a **dbo.SqlView.Column** for the agent running the agent procedure. See **System > Database Views** (page 472) for a list of the SQL views and columns that are available.

**Note: SQL View Data** - This older method of returning a database view value is only necessary if you are trying to return a value from a *different machine than the machine running the agent procedure*.

Use the **GetVariable** command with the **SQL View Data** option to create a new procedure variable and set it to the value of a `dbo.SqlView.Column` value. Use the format `SqlViewName/ColumnName/mach.groupID` or `SqlViewName/ColumnName`. If the optional machine ID is omitted, then the value for the agent executing the procedure is retrieved. If `ColumnName` contains a space, surround it with square brackets. Example: `vSystemInfo/[Product Name]`. See **System > Database Views** (page 472) for a list of the SQL views and columns that are available.

- **Automatic Administrator Variables** - Three administrator variables are declared automatically. These automatic administrator variables allow agent procedures to access values not present from an SQL view.
  - ✓ `#adminDefaults.adminEmail#` - Email address of the VSA user who scheduled the agent procedure.
  - ✓ `#adminDefaults.adminName#` - Name of the VSA user who scheduled the agent procedure.
  - ✓ `#scriptIdTab.scriptName#` - Name of the agent procedure.
- **WMI Property** - A WMI namespace, class, and property. The format of the specified WMI property is `NameSpace:Class.Property`. For example, `root\cimv2:Win32_OperatingSystem.FreePhysicalMemory`. Specify an instance using the following syntax: `NameSpace:Class[N].Property` where [N] is the instance number. For example, `root\cimv2:Win32_OnboardDevice[3].Description`. The first instance may be specified with or without specifying the [1] instance number.
- **Expression Value** - Specify an expression that consists of procedure variables and six mathematical operators `+`, `-`, `*`, `/`, `(`, and `)` that are evaluated and assigned to a new procedure variable. For example, `((#variable1# + #variable2#) + 17.4) / (#variable3# * 4)`. The procedure variables must contain numeric values.
- **64-Bit Registry Value** - Data from the specified registry value on the managed machine.
- **Prompt when procedure is scheduled** - Displays a message prompt to enter a value when an agent procedure is run. The value is stored in the variable name you specify. Specify the prompt text and variable name. For example, each time this procedure is run, a VSA user could enter a different machine directory.
- **Windows Environment Variables** - You can reference Windows environmental variables within the **Execute File**, **Execute File in Path** and **Execute Shell Commands** only. Enclose the whole command in quotes, because the environmental variable may contain spaces which might affect execution. For other agent procedure commands, use **Get Variable** to get the registry key containing the environmental variables, located under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment`.

## Variable Manager

Use the **Variable Manager** to define variables that can be used repeatedly in different agent procedures. You can maintain multiple values for each managed variable, with each value applied to one or more group IDs. Managed variables cannot be re-assigned new values within a procedure. Within a procedure, reference a managed variable by bracketing the variable name with the `<` and `>` character. Example: `<VariableName>`. See **Using Variables** (page 115).

Using managed variables, managed machines can run agent procedures that access *locally available resources* based on the group ID or subgroup ID.

**Note:** Using [System > Naming Policy \(page 395\)](#), this benefit can be applied automatically by IP address even to a highly mobile workforce that travels routinely between different enterprise locations.

### Select Variable

Select a variable name from the drop-down list or select `<New Variable>` to create a new variable. Variable names are **case sensitive**.

### Rename/Create Variable

Enter a new name for the new variable you are creating or for an existing variable you are renaming. Select the delete icon  to delete the entire variable from all groups.

### Public

Selecting the **Public** radio button allows the variable to be used by all users. However, only master role users can create and edit shared variables.

### Private

Selecting the **Private** radio button allows the variable to be used only by the user who created it.

### Apply

Enter the initial value for a variable. Then select one or more **Group IDs** and click **Apply**. Empty values are not allowed.

### Remove

Select one or more group IDs, then click **Delete** to remove the value for this variable from the group IDs it is assigned to.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Group ID

Displays all group IDs the logged in user is authorized to administer.

### Value

Lists the value of the variable applied to the group ID.

## Manage Files Stored on Server

[Agent Procedures > Schedule / Create > Manage Files](#)

- This page applies to the following product: [On Premises](#)

Use the **Manage Files Stored on Server** popup window to upload a file and store it on the KServer. You can also list, display and delete files already stored on the KServer. Agent procedures can distribute these files to managed machines using the **Write File** or **Write File in Directory Path** commands.

**Note:** This store of files is not machine-specific. [Get File \(page 127\)](#) uploads and stores machine-specific files on the server.

To upload a file:

- Click **Private files** or **Shared files** to select the folder used to store uploaded files. Files stored in the **Private files** folder are not visible to other users.

- Click **Browse...** to locate files to upload. Then click **Upload** to upload the file to the KServer.

To delete a file stored on the KServer:

- Click **Private files** or **Shared files** to select the folder used to store uploaded files.
- Click the delete icon  next to a file name to remove the file from the KServer.

**Note:** An alternate method of uploading files is to copy them directly to the managed files directory on the IIS server. This directory is normally located in the `C:\Kaseya\WebPages\ManagedFiles` directory. In that directory are several sub-directories. Put private files into the directory named for that user. Put shared files into the `VSASharedFiles` directory. Any files located in this directory will automatically update what is available in the **Manage Files Stored on Server** user interface at the next user logon.

## Folder Rights

### Private Folders

Objects you create—such as reports, procedures, or monitor sets—are initially saved in a folder with your user name underneath a **Private** cabinet. This means only you, the creator of the objects in that folder, can view those objects, edit them, run them, delete them or rename them.

To share a private object with others you first have to drag and drop it into a folder underneath the **Shared** cabinet.

**Note:** A master role user can check the **Show shared and private folder contents from all users** checkbox in **System > Preferences** (page 391) to see all shared and private folders. For Private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

### Shared Folders

The following **Share Folder** guidelines apply to folders underneath a **Shared** cabinet:

- If the **Apply share rights from parent folder** checkbox in the **Share Folder** dialog box is checked, a folder's share rights are determined by the parent folder. Otherwise, the folder's share rights can be set independently from the parent.
- If you have rights to delete a folder, deleting that folder deletes all objects and subfolders as well, regardless of share rights or ownership assigned to those subfolders.

**Note:** Scopes have nothing to do with the visibility of folders and objects in a folder tree. Scopes limit what your folder objects can work with. For example, you can be shared folders containing reports, procedures or monitor sets but you will only be able to use these objects on machine groups within your scope.

- To set share rights to a folder, select the folder, then click the **Share Folder** button to display the **Share Folder** dialog.
  - You can share specific rights to a folder with any individual user or user role you have visibility of. You have visibility of:
    - ✓ Any user roles you are a member of, whether you are currently using that user role or not.
    - ✓ Any individual users that are members of your current scope.
  - Adding a user or user role to the **Shared Pane** allows that user to run any object in that folder. No additional rights, including **View**, have to be assigned to the user or user role to run the object.
  - Checking any *additional rights*—such as **View**, **Edit**, **Create**, **Delete**, **Rename**, or **Share**—when you add the user or user role provides that user or user role with those additional rights. You

have to remove the user or user role and re-add them to make changes to their additional rights.

- **View** does not refer to being able to view the folder. If you assign a user to the share folder without giving the user the **View** right, the user must still be able to see the folder and its objects to be able to select and run the object. Instead **View** means the user or user role can display the details of the object and export it, beyond just running the object.
- **Share** means the user or user role can assign share rights for a selected folder using the same **Share Folder** dialog box you used to assign them share rights.

### Take Ownership

Users are always the one and only owner of their **Private** folders. **Shared** folders are also *owned* and are only owned by one user at a time. Ownership of a shared folder provides "full rights" to a folder's objects, *regardless of the share rights assigned to that user*. When you first create a shared folder, either as a master role user or a non-master role user, you are the owner of that shared folder.

Master role users have an additional right, called **Take Ownership**, that allows them to take ownership of any **Shared** folder that is visible in the folder tree.

**Note:** A master role user can check the **Show shared and private folder contents from all users in System > Preferences** (page 391) to see all shared and private folders. For **Private** folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

As a master role user, if the  **Take Ownership** button displays when you select a **Shared** folder, that means you're not the owner of that folder. If a folder you don't own has been shared with you, then several other buttons may display alongside the  **Take Ownership** button. Until you click the  **Take Ownership** button you're restricted to the actions determined by the share rights you've been assigned.

Clicking the  **Take Ownership** button makes you the one and only owner of that shared folder. Taking ownership displays an orange dot on the folder , indicating ownership. Ownership overrides your assigned shared rights and gives you complete access to:

- Add, edit, change, rename or delete objects in that folder.
- Add, rename or delete subfolders.
- Rename or delete the folder you took ownership of and all its contents.

Typically the reason you take ownership of a shared object is to maintain its contents because the original owner can't do so. For example, the owner of a shared object may have left the company and no longer be available. In most cases, master role users can work within the share rights they've been assigned by other VSA users.

**Note:** Deleting a VSA user from the system assigns ownership of all objects belonging to that VSA user to the VSA user performing the delete.

---

## Distribution

### Agent Procedures > Distribution

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Distribution** page spreads network traffic and server loading by executing agent procedures evenly throughout the day or a specific block of time in a day. Applies to agent procedures currently scheduled to run on a **recurring basis** only.

**Note:** Recurring procedures listed here include function-specific procedures *that are not visible as agent procedures in the Schedule / Create (page 94) folder tree*, such as procedures created using a Patch Management wizard.

Procedures can cause excessive network loading by pushing large files between the KServer and agent. Performing these operations with hundreds of agents simultaneously may cause unacceptable network loading levels.

## Procedure Histograms

The system plots a histogram for each procedure currently scheduled to run on a recurring basis. Setting the histogram period to match the recurring interval of the procedure counts how many machines execute the procedure in a specific time interval. Peaks in the histogram visually highlight areas where a lot of machines are trying to execute the procedure at the same time. *Click a peak to display a popup window listing all machine IDs contributing to that peak load.* Use the controls, described below, to reschedule the procedure such that the network loading is spread evenly over time. **Only machine IDs currently matching the Machine ID / Group ID filter are counted in the histogram.**

### Reschedule selected procedure evenly through the histogram period

Pick this radio control to reschedule selected procedures running on all machines IDs currently matching the **Machine ID / Group ID filter** (page 26). Procedure execution start times are staggered evenly across the entire histogram period.

### Reschedule selected procedure evenly between <start time> and <end time>

Pick this radio control to reschedule selected procedures running on all machines IDs currently matching the Machine ID / Group ID filter. Procedure execution start times are staggered evenly, beginning with the start time and ending with the end time.

### Run recurring every <N> <periods>

This task is always performed as a recurring task. Enter the number of times to run this task each time period.

### Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

### Distribute

Click the **Distribute** button to schedule selected procedures, using the schedule parameters you've defined.

**Note:** The procedure recurring interval is replaced with the histogram period.

### Select Histogram Period

Selects the schedule time period to display histograms.

### Histogram Plots

Each recurring procedure displays a histogram of all the machine IDs that are scheduled to run that procedure within the selected histogram period. Only machine IDs currently matching the Machine ID / Group ID filter are counted in the histogram.

Above the histogram is a:

## Agent Procedures

- **Procedure name** - name of the procedure. Check the box next to the procedure name to select this procedure for distribution.
- **Peak** - the greatest number of machines executing the procedure at the same time.
- **Total** - total number of machines executing the procedure.

---

# Agent Procedure Status

## Agent Procedures > Agent Procedure Status

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center*
- Similar information is displayed in the Pending Procedures tab of the Live Connect (*page 380*) and Machine Summary (*page 137*) pages.

The **Agent Procedure Status** page displays the status of agent procedures for a selected machine ID. The list of machine IDs you can select is based on the **Machine ID / Group ID filter** (*page 26*). Users can, at a glance, find out what time a agent procedure was executed and whether it was successfully executed. See Agent Procedures > **Schedule / Create** (*page 94*) for more information about agent procedures.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (*page 583*).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (*page 592*) displayed is based on the **Machine ID / Group ID filter** (*page 26*) and the machine groups the user is authorized to see using System > User Security > **Scopes** (*page 404*).

## Procedure Name

The name of the agent procedure.

## Time

The date and time the agent procedure was last executed.

## Status

Displays the results of the executed agent procedure. Overdue date/time stamps display as **red text with yellow highlight**. Recurring agent procedures display as **red text**.

## Admin

Displays the VSA user who scheduled the agent procedure.

---

# Patch Deploy

## Agent Procedures > Patch Deploy

- This page applies to the following product: On Premises

The **Patch Deploy** wizard is a tool that creates an agent procedure to distribute and apply Microsoft patches. The wizard walks you through a step by step process resulting in an agent procedure you can schedule, to deploy a patch to any managed machine.

Microsoft releases many hot fixes as patches for very specific issues that are not included in the Microsoft Update Catalog or in the Office Detection Tool, the two patch data sources the **Patch Management** module uses to manage patch updates. **Patch Deploy** enables customers to create a patch installation procedure for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

See **Methods of Updating Patches** (page 306), **Configuring Patch Management** (page 306), **Patch Processing** (page 307), **Superseded Patches** (page 307), **Update Classification** (page 308) and **Patch Failure** (page 308) for a general description of patch management.

### Step 1: Enter 6-digit knowledge base article number.

Microsoft publishes a vast assortment of information about its operating system in the **Microsoft Knowledge Base**. Each article in the Knowledge Base is identified with a 6-digit Q number (e.g. Q324096.) All Microsoft patches have an associated knowledge base article number.

**Note:** Entering the article number is optional. Leave it blank if you do not know it.

### Step 2: Select the operating system type.

Sometimes patches are specific to a certain operating system. If the patch you are trying to deploy applies to a specific OS only, then select the appropriate operating system from the drop-down control. When the wizard creates the patch deploy procedure, it restricts execution of the procedure to only those machines with the selected OS. This prevents inadvertent application of operating system patches to the wrong OS.

### Step 3: Download the patch.

This step is just a reminder to fetch the patch from Microsoft. Typically there is a link to the patch on the knowledge base article describing the patch.

### Step 4: How do you want to deploy the patch?

The Patch Deploy wizard asks you in step 4 if you want to **Send the patch from the KServer to the remote machine and execute it locally** or **Execute the patch from a file share on the same LAN as the remote machine**. Pushing the patch down to each machine from the VSA may be bandwidth intensive. If you are patching multiple machines on a LAN no internet bandwidth is used to push out the patch. Each machine on the LAN can execute the patch file directly from a common file share.

### Step 5: Select the patch file or Specify the UNC path to the patch stored on the same LAN as the remote machine.

If **Send the patch from the KServer to the remote machine and execute it locally** was selected, then the patch must be on the VSA server. Select the file from the drop-down list.

**Note:** If the patch file does not appear in the list then it is not on the KServer. Click the **Back** button and upload the file to the KServer by clicking the **first here** link.

If **Execute the patch from a file share on the same LAN as the remote machine** was selected, then the patch must be on the remote file share prior to running the patch deploy procedure. The specified path to the file must be in **UNC format** such as `\\computername\dir\`.

**Note:** If the file is not already on the remote file share, you can put it there via FTP. Click the **Back** button and then the **second here** link takes you to FTP.

### Step 6: Specify the command line parameters needed to execute this patch silently.

To deploy a patch silently you need to add the appropriate command line switches used when executing the patch. Each knowledge base article lists the parameters for **silent install** (page 597). Typical switch settings are `/q /m /z`.

**Note:** Command line parameters are optional. Leave it blank if you do not know it.

### Step 7: Name the procedure.

Enter a name for the new agent procedure you can run to deploy the patch.

### Step 8: Reboot the machine after applying the patch.

Check this box to automatically reboot the managed machine after applying the patch. The default setting is to *not* reboot.

### Click the **Create** button.

A new agent procedure is created. Use Agent Procedure > **Schedule / Create** (page 94) to display the new agent procedure in the folder tree, under your private folder user name. You can run this new agent procedure to deploy the patch to any managed machine.

---

## Application Deploy

### Agent Procedures > Application Deploy

- This page applies to the following product: On Premises

The **Application Deploy** page is a wizard tool that creates an agent procedure to distribute vendor installation packages, typically `setup.exe`. The wizard walks you through a step by step process resulting in an agent procedure you can schedule, to deploy an application to any managed machine.

### Deploying Software Vendor's Install Packages

Most vendors provide either a single file when downloaded from the web or set of files when distributed on a CD. Executing the installer file, typically named `setup.exe` or `abc.msi`, installs the vendor's application on any operating system.

The **Application Deploy** wizard takes you through an interview process to determine the type of installer and automatically generates a procedure to deploy install vendor packages.

The VSA provides a small utility to automatically identify all supported installer types. Download and run `kInstId.exe` to automatically identify the installer type.

**Note:** See **Creating Silent Installs** (page 125) to ensure vendor installation packages don't pause for user input during installation.

### Step 1: How do you want to deploy the application?

The wizard generated procedure tells the managed machine where to get the application installation file to execute. The **Application Deploy** wizard asks you in step 1 if you want to **Send the installer from the**

**VSA server to the remote machine and execute it locally** or **Execute the installer from a file share on the same LAN as the remote machine.**

Pushing the application installation file to each machine from the VSA may be bandwidth intensive. If you are installing to multiple machines on a LAN no internet bandwidth is used to push out the application installation file. Each machine on the LAN can execute the application installation file directly from a common file share.

**Step 2: Select the application install file or Specify the UNC path to the installer stored on the same LAN as the remote machine.**

If **Send the installer from the VSA server to the remote machine and execute it locally** was selected, then the installer file must be on the VSA server. Select the file from the drop-down list.

**Note:** If the installer file does not appear in the list then it is not on the VSA server. Click the [here](#) link to upload the file to the server.

If **Execute the installer from a file share on the same LAN as the remote machine** was selected, then the installer file must be on the remote file share prior to running the application deploy procedure. The specified path to the file must be in **UNC format** such as `\\computername\dir\`.

**Note:** If the file is not already on the remote file share, you can put it there via FTP. Click the [here](#) link to start FTP.

**Step 3: What kind of installer is this?**

The wizard need to know what kind of installer was used by your software vendor to create the install package. The VSA provides a small utility to automatically identify all supported installer types. Download and run `kInstId.exe` to automatically identify the installer type. Supported installer types are:

- Windows Installer (MSI files)
- Wise Installer
- Installshield - Package For The Web
- Installshield - Multiple Files
- Other

**Step 4: Name the agent procedure.**

Enter a name for the new agent procedure you can run to install the application.

**Step 5: Reboot the machine after installing the application.**

Check this box to automatically reboot the managed machine after running the install. The default setting is to *not* reboot.

**Click the Create button.**

A new agent procedure is created. Use Agent Procedure > **Schedule / Create** (*page 94*) to display the new agent procedure in the folder tree, under your private folder user name. You can run this new agent procedure to install the application to any managed machine.

## Creating Silent Installs

Most vendors provide either a single file, when downloaded from the web, or set of files, when distributed on a CD. Executing the installer file, typically named `setup.exe`, installs the vendor's application on any operating system. Vendors typically use one of three applications to create install packages: **InstallShield**, **Windows Installer**, or **Wise Installer**. Each of these applications provides a method

for creating **silent installs** (page 597). When automating the installation of vendor install packages, you'll want to ensure the installation package does not pause for user input during installation.

### Silent Installs with InstallShield

InstallShield has a record mode that captures answers to all dialog boxes in the installation procedure. InstallShield requires the recorded response `iis` file to be on the managed machine during the installation. To deploy, the agent procedure must use the **Write File** command to send both the `setup.exe` and `record.iis` files from VSA server to the managed machine and then use **Execute File** to run `setup.exe` with the options `/s /f"<path>\record.iis"`. Refer to your InstallShield help guide for more information regarding the silent installation capability with a recorded response file.

Create a custom install package by following these steps:

1. Verify the install package was made with InstallShield.
  - a. Launch the install package.
  - b. Confirm `InstallShield Wizard` displays at the end of the window title bar.
2. Launch the install package in record mode from a command prompt.
  - a. **If the install package is a single file** - Run `setup.exe /a /r /flc:\temp\record.iis`. `Setup.exe` is the name of the install package. `c:\temp\record.iis` is the full path filename to save the recorded output.
  - b. **If the install package is a set of files** - Run `setup.exe /r /flc:\temp\record.iis`. `Setup.exe` is the name of the install package. `c:\temp\record.iis` is the full path filename to save the recorded output.
3. Deploy the install package with the recorded dialog box responses. Use the **Write File** agent procedure command to copy both the vendor's install package and `record.iis` file to each managed machine or to a file server accessible by each managed machine.
4. Execute the install package with silent mode command line parameters using the **Execute File** procedure command.
  - a. **If the install package is a single file** - Run `setup.exe /s /a /s /flc:\temp\record.iis`. `Setup.exe` is the name of the install package. `c:\temp\record.iis` is the full path filename location of the recorded settings.
  - b. **If the install package is a set of files** - Run `setup.exe /s /flc:\temp\record.iis`. `Setup.exe` is the name of the install package. `c:\temp\record.iis` is the full path filename location of the recorded settings.

### Silent Installs with Windows Installer

Windows Installer does not have a record mode. As such it can only silently install the **Typical** install configuration. To silently install a Windows Installer package write a procedure to perform the following:

1. Use the **Write File** agent procedure command to copy the vendor's install package to each managed machine or to a file server accessible by each managed machine.
2. Run the install package with the `/q` parameter using the **Execute File** agent procedure command.

### Silent Installs with Wise Installer

Wise Installer does not have a record mode. As such it can only silently install the **Typical** install configuration. To silently install a Wise Installer package write a procedure to perform the following:

1. Use the **Write File** agent procedure command to copy the vendor's install package to each managed machine or to a file server accessible by each managed machine.
2. Run the install package with the `/s` parameter using the **Execute File** agent procedure command.

---

# Packager

## Agent Procedures > Packager

- This page applies to the following product: On Premises

The **Packager** is a wizard tool used to create a package when a pre-defined install solution cannot be used. **Packager** evaluates the state of a source machine before and after an installation and/or resource change. The **Packager** compiles the differences into a single executable file—the **package**—that can be distributed via agent procedures to any managed machine. Distribute a package any way you choose. You can email it, or store it on a server where a **custom procedure** (*page 94*) can perform a silent installation on any managed machine.

### Step 1: Download the Packager application to the machine you plan to build your install package on.

For best results, we recommend you create a package on a representative machine; that is, a machine that closely resembles the managed machines on which the package will be deployed.

**Each Package is OS dependent.** To deploy to multiple operating systems, you need to build a package for each OS. During installation, **Packager** checks the target machine's operating system and does not continue if the package is being deployed on an OS different than the source OS.

### Step 2: Execute Packager.exe and follow the on-screen instructions to create a distribution package.

The following tasks are performed:

1. **Packager** takes a snapshot of the source system.
2. Install any application and/or resource on the source system.
3. Execute **Packager** again. **Packager** records the changes in the source system and creates a package.

**Packager** picks up everything you do to a machine between the time you take the first snapshot and create the package. Be careful what additional tasks you perform on the source machine as any system changes will be rolled into the package. Close all applications before running **Packager**. This prevents open applications from modifying the system during package creation.

### Step 3: Distribute the package via a procedure.

Use Agent Procedure > **Schedule / Create** (*page 94*) to create an agent procedure that downloads the package to managed machines and runs it. Packages can only be executed on machines with agents installed. If the package fails to install, **Packager** has complete rollback capability. The rollback executable and associated restore files are located in the agent directory on the target machine in the directory `C:\Program Files\Kaseya\KPackage`.

---

# Get File

## Agent Procedures > Get File

- This page applies to the following product: On Premises

The **Get File** page accesses files previously uploaded from a managed machine. Files can be uploaded to a machine-specific directory on the KServer using the **Get File** or **Get File In Directory Path** commands. Clicking the machine ID displays *all* uploaded files for that machine ID. Click the link underneath a file to display the file or run it.

**Note:** The files stored on the KServer using the **Get File** command are machine-specific. Use **Manage Files Stored on Server** (page 118) to access files stored on the KServer that are not machine-specific.

- Each file is displayed as a link. Click any filename to access that file.
- Remove files by clicking the delete icon  next to the file.

### Example 1: Checking Large Number of Managed Machines Simultaneously

**Get File** is designed to support automated checks on a large number of managed machines simultaneously.

**Note:** If all you want to do is get a file from a managed machine as a one-time event then **Remote Control > FTP** (page 370) is the simplest way.

Use **Get File** in conjunction with an agent procedure to perform some automated task on a set of managed machines. For example, if you have a utility that reads out some information unique to your client computers you can write a procedure to do the following:

1. Send the utility to the managed machine using either the **Write File** procedure command or the **Distribute File** page.
2. Execute the utility using either the **Execute Shell Command** or **Execute File** agent procedure command and pipe the output to a text file, such as `results.txt`.
3. Upload the file to the KServer using the **Get File** command.

### Example 2: Comparing Versions of a File

As an option in the **Get File** agent procedure command, existing copies of uploaded files can be renamed with a `.bak` extension prior to the next upload of the file. This allows you to examine both the latest version of the file and the previous version. For example, use the **IF-ELSE-STEP** agent procedure editor to create a simple **Get File** agent procedure.

The first time the **Get File** agent procedure command executes on a managed machine the agent sends `c:\temp\info.txt` to the KServer and the KServer stores it as `news\info.txt`. The second time **Get File** agent procedure executes, the KServer renames the original copy of `news\info.txt` to `news\info.txt.bak` then uploads a fresh copy and saves it as `news\info.txt`.

Also as an option, an email alert can be sent when a change in the uploaded file has been detected, compared to the last time the same file was uploaded. The **Get File** command must have either the **Overwrite existing file and send alert if file changed** setting or the **Save existing version, get file, and send alert if file changed** setting selected.

### Example 3: Get File Changes Alerts

To perform continuous health checks on managed machines, run the agent procedure on a recurring schedule and activate a **Get File Changes** alert using **Monitor > Alerts - Get Files** (page 227). The VSA instantly notifies you of any changes to the results.

### Troubleshooting Patch Installation Failures

When patch scan processing reports patch installations have failed, a `KBxxxxxxx.log` (if available) and the `WindowsUpdate.log` are uploaded to the KServer. Additionally, for those patches that required an "Internet based install", a `ptchdlin.xml` file will be uploaded to the KServer. These files can be reviewed using **Agent Procedures > Get File** (page 127) for a specific machine and can help you troubleshoot patch installation failures. **Info Center > Reports > Logs > Agent Procedure Log** contains entries indicating these log files have been uploaded to the KServer for each machine.

---

# Distribute File

## Agent Procedures > Distribute File

- This page applies to the following product: On Premises

The **Distribute File** function sends files stored on your VSA server to managed machines. It is ideal for mass distribution of configuration files, such as virus foot prints, or maintaining the latest version of executables on all machines. The VSA checks the integrity of the file every **full check-in** (page 588). If the file is ever deleted, corrupted, or an updated version is available on the VSA, the VSA sends down a new copy prior to any procedure execution. Use it in conjunction with recurring procedures to run batch commands on managed machines.

**Note:** The procedure command `Write File` performs the same action as **Distribute File**. Each time a procedure executes the `Write File` command, the agent checks to see if the file is already there or not. If not, the file is written. `Write File` is better than **Distribute File** for sending executable files you plan to run on managed machines using agent procedures.

### Select server file

Select a file to distribute to managed machines. These are the same set of files managed by clicking the **Manage Files...** link on this page.

**Note:** The only files listed are your own private managed files or shared managed files. If another user chooses to distribute a private file you can not see it.

### Specify full path and filename to store file on remote machine

Enter the path and filename to store this file on selected machine IDs.

### Manage Files...

Click the **Manage Files** (page 118)... link to display the **Manage Files Stored on Server** popup window. Use this window to add, update, or remove files stored on the KServer. This same window displays when you click the **Managed Files** button using **Schedule / Create** (page 94). Private files are listed with (Priv) in front of the filename.

### Distribute

Click the **Distribute** button to start distribution management of the file selected in **Select server file** and write it to the location specified in **Specify full path and filename to store file on remote machine**. This effects all checked machine IDs.

### Clear

Click the **Clear** button to remove the distribution of the file selected in **Select server file** from all checked machine IDs.

**Warning:** **Clear** and **Clear All** do *not* delete the file from either managed machines or the KServer. These functions simply stop the integrity check and update process from occurring at each full check-in.

### Clear All

**Clear All** removes all file distributions from all checked managed machines.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Agent Procedures

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Server File

The name of the file being distributed.

### Agent File Location

The target directory on the managed machine. To the left of each target file location for a specific machine ID are two icons. Click  to cancel that file distribution for that machine ID. Click  to edit the destination path and filename for that machine ID.

## Chapter 5

# Audit

### In This Chapter

Audit Overview	133
Run Audit	134
Audit Summary	135
Configure Column Sets	137
Machine Summary	137
System Info	140
Installed Applications	141
Add/Remove	142
Software Licenses	143
Documents	143

## **Audit**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Audit Overview

## Audit

**Agents** (page 583) can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the KServer so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machines's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > **Reports** (page 149) are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 219) types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**. Collected audit information includes:

- All hardware, including CPUs, RAM, PCI cards, and disk drives.
- All installed software, including licenses, version numbers, full path, and description.
- System Information from DMI and SMBIOS including PC make, model, serial number, mother board type, and over **40** other pieces of information describing the PC and its configuration.
- OS info with version number and service pack build.
- Current network settings including local IP address, gateway IP address, DNS, WINS, DHCP, and MAC address.

---

Functions	Description
<b>Run Audit</b> (page 134)	Schedules latest, system, and baseline audits of machine IDs.
<b>Audit Summary</b> (page 135)	Displays data returned by audits of machines
<b>Configure Column Sets</b> (page 137)	Configures columns sets for the Audit Summary page.
<b>Machine Summary</b> (page 137)	Displays detailed information about a single managed machine.
<b>System Information</b> (page 140)	Shows DMI / SMBIOS data collected.
<b>Installed Applications</b> (page 141)	Shows a list of executable (.exe) files on selected managed machines.
<b>Add/Remove</b> (page 142)	Shows the Add or Remove Programs list from a managed machine.
<b>Software Licenses</b> (page 143)	Shows a list of vendor license codes found on selected managed machines.
<b>Documents</b> (page 143)	Stores files associated with a machine ID.

---

---

# Run Audit

## Audit > Run Audit

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Run Audit** page performs audits of the hardware and software configuration of managed machines.

## Audits

**Agents** (page 583) can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the KServer so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machine's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > **Reports** (page 149) are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 219) types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**.

**Note:** PCI & Disk H/W audits are performed automatically on Windows XP and later operating systems. Older systems are not supported.

## Actions

**Schedule Audit** - Click **Schedule Audit** or **Reschedule Audit** to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

- **Baseline Audit, Latest Audit** or **System Information** - Type of audit.
- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.
- **Reschedule Audit** - Populates the scheduler with the values of a pending schedule so you can make adjustments.
- **Run Audit Now** - Schedules an audit to run immediately.
- **Cancel Audit** - Cancels a scheduled audit.

## Remind me when accounts need audit scheduled

If checked, displays a pop up warning message if audits have not been scheduled for one or more machine IDs. The warning displays each time you select **Run Audit**. Applies to each VSA user individually.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Machine.Group ID

The top line shows the machine ID. The bottom line displays the last time a System Info audit was performed. Overdue date/time stamps display as **red text with yellow highlight**. Pending and completed date/time stamps display as black text.

## System Information / Latest Audit / Baseline Audit

Each column displays the last time that type of audit was performed. Overdue date/time stamps display as **red text with yellow highlight**. Pending and completed date/time stamps display as black text.

## Next Audit

Displays the time of the next scheduled Latest Audit. Overdue date/time stamps display as **red text with yellow highlight**. Pending and completed date/time stamps display as black text.

## Recurring Interval

Displays the recurring interval for latest audits.

---

# Audit Summary

## Audit > Audit Summary

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The Audit > **Audit Summary** page provides a view of the data returned by audits of machines using the **Run Audit** (page 134) page. The columns of audit data shown on this page are individually selectable and filterable. User-defined sets of columns can also be selected. Columns sets are defined using the **Configure Column Sets** (page 137) page. Additional data not shown in the **Audit Summary** page is provided using the **Machine Summary** (page 137) page. This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).

## Audit

Columns of audit data, in the default order they display in this page, include:

- **Machine ID** - Machine ID label used throughout the system.
- **Current User** - Logon name of the machine user currently logged into the machine (if any).
- **Last Reboot Time** - Time of the last known reboot of the machine.
- **Last Checkin Time** - Most recent time when a machine checked into the KServer.
- **Group ID** - The group ID portion of the machine ID.
- **First Checkin Time** - Time when a machine first checked into the KServer.
- **Time Zone** - The time zone used by the machine.
- **Computer Name** - Computer name assigned to the machine.
- **Domain/Workgroup** - The workgroup or domain the computer belongs to.
- **DNS Computer Name** - The fully qualified DNS computer name for the machine, which comprises the computer name plus the domain name. For example: `jsmithxp.acme.com`. Displays only the computer name if the machine is a member of a workgroup.
- **Operating System** - Operation system type the machine is running.
- **OS Version** - Operation system version string.
- **CPU Type** - Processor make and model.
- **CPU Speed** - Clock speed of the processor.
- **CPU Count** - The number of CPUs.
- **RAM (MB)** - Megabytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine.
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **Primary/Secondary KServer** - IP address / name the machine uses to communicate with the KServer.
- **Quick Checkin Period - Quick check in** (*page 588*) time setting in seconds.
- **Contact Name** - Machine user name entered in **Edit Profile** (*page 79*).
- **Contact Email** - Email address entered in Edit Profile.
- **Contact Phone** - Phone number entered in Edit Profile.
- **Manufacturer** - System manufacturer.
- **Product Name** - System product name.
- **System Version** - Product version number.
- **System Serial Number** - System serial number.
- **Chassis Serial Number** - Serial number on the enclosure.
- **Chassis Asset Tag** - Asset tag number on the enclosure.
- **External Bus Speed** - Motherboard bus speed.
- **Max Memory Size** - Max memory size the motherboard can hold.
- **Max Memory Slots** - Total number of memory module slots available.
- **Chassis Manufacturer** - Manufacturer of the enclosure.
- **Chassis Type** - Enclosure type.
- **Chassis Version** - Enclosure version number.
- **Motherboard Manufacturer** - Motherboard manufacturer.
- **Motherboard Product** - Motherboard product ID.
- **Motherboard Version** - Motherboard version number.
- **Motherboard Serial Num** - Motherboard serial number.
- **Processor Family** - Processor type installed.
- **Processor Manufacturer** - Processor manufacturer.
- **Processor Version** - Processor version ID.
- **CPU Max Speed** - Max processor speed supported.
- **CPU Current Speed** - Speed processor is currently running at.
- **IPv4 Address** - IP address assigned to the machine, in version 4 format.

- **IPv6 Address** - IP address assigned to the machine, in version 6 format.
- **Subnet Mask** - Networking subnet assigned to the machine.
- **Default Gateway** - Default gateway assigned to the machine.
- **Connection Gateway** - IP address seen by the KServer when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
- **Country** - The country associated with the Connection Gateway.
- **MAC Address** - MAC address of the LAN card used to communicate with the KServer.
- **DNS Server** - IP address of the DNS server assigned to the machine.
- **DHCP Server** - The IP address of the DHCP server used by this machine.
- **Primary/Secondary WINS** - WINS settings.
- **Free Space** - The free data storage space in gigabytes.
- **Used Space** - The used data storage space in gigabytes.
- **Total Size** - The total data storage space in gigabytes.
- **Number of Drives** - The number of drives on the machine.
- **Portal Access Logon** - Logon name given to a machine user for logging into the KServer.
- **Portal Access Remote Control** - Enabled if this machine user can log in and get remote control access *to their own machine from another machine*. Disabled if access is denied.
- **Portal Access Ticketing** - Enabled if this machine user can log in and enter trouble tickets. Disabled if access is denied.
- **Portal Access Chat** - Enabled if this machine user can *initiate* chat sessions with a VSA user. Disabled if access is denied.

---

## Configure Column Sets

### Audit > Configure Column Sets

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Configure Columns Sets** page defines columns sets that can be used to select a set of columns in the Audit > **Audit Summary** (*page 135*) table.

### Actions

- **New** - Create a new column set.
- **Edit** - Edit a selected column set.
- **Delete** - Delete a selected column set.

### Select a Column Set

Select an existing column set in the middle panel of this page. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

---

## Machine Summary

### Audit > Machine Summary

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*
- Similar information is provided using Info Center > Reporting > **Machine Summary** (*page 154*).

## Audit

### Machine Summary

The **Machine Summary** page allows users to perform tasks and functions solely for one managed machine. A series of tabbed property sheets provided access to various categories of information about the managed machine.

### Actions

You can maintain an unlimited number of custom fields of information about managed machines. Custom fields can be maintained on both the **Summary** tab and the Hardware > **Summary** tab of this page. Custom fields can also be maintained on the Audit > **System Information** (page 140) page.

- **New Custom Field** - Creates a new custom field.
- **Rename Custom Field** - Renames a custom field.
- **Delete Custom Field** - Deletes a custom field.

### Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

### Summary

- **Collections** - Displays the **collections** (page 588) a machine is a member of. Defined using the **Only show selected machine IDs** option in **View Definitions** (page 28).
- **Name/OS Information** - Displays the name, operating system and OS version.
- **System Information** - Displays the manufacturer of system, the product name, version and serial number.
- **Network Information** - Displays network configuration settings.
- **CPU/RAM Information** - Displays CPU and RAM specifications.
- **Custom Fields** - Displays custom fields and values assigned by the user to this machine.

### Software

- **System Information** - Lists system hardware attributes and related information.
- **Software Licenses** - Lists all software licenses found for a selected machine ID. Duplicate license keys found on more than one machine **display in red text**. Clicking the number link next to the title of a duplicate license lists the machine IDs using the duplicate license.
- **Installed Applications** - Lists all the applications installed on the managed machine.
- **Add/Remove** - Displays programs listed in Add/Remove window of Windows machines.

### Hardware

- **Summary**
  - **System Information** - Lists system hardware attributes and related information.
  - **Network Information** - Displays network configuration settings.
  - **Chassis** - The chassis manufacturer, type, version, serial number and asset tag.
  - **Motherboard** - The motherboard manufacturer, product, version, serial number and external bus speed.
  - **CPU/RAM Information** - Displays CPU and RAM specifications.
  - **Custom Fields** - Displays custom fields and values assigned by the user to this machine.
- **Printers** - Lists the printers and ports a machine can direct print jobs to.
- **PCI & Disk Hardware** - Displays type, vendor, and product names.
- **Disk Volumes** - Displays disk volume information.
- **Disk Partitions** - Displays the partitions on each disk volume.

- **Disk Shares** - Displays shared folders.

### Agent

- **Settings** - Displays information about the agent on the managed machine:
  - **Agent version**
  - **Current User**
  - **Last check-in**
  - **Last reboot**
  - **First time check-in**
  - **Patch Policy Membership** - Defined using Patch Management > **Membership: Patch Policy** (page 327)
  - **View Definition Collections** - Defined using the **Only show selected machine IDs** option in **View Definitions** (page 28).
  - **Working Directory** - Can also be defined using Agent > **Working Directory** (page 78).
  - **Check-In Control** - Can also be defined using Agent > **Check-In Control** (page 75).
  - **Edit Profile** - Can also be defined using Agent > **Edit Profile** (page 79).
  - **Agent Logs and Profiles** - Can also be defined using Agent > **Log History** (page 35).
- **Logs** - Displays the logs available for a machine: Alarm Log, Monitor Action Log, Agent Log, Configuration Changes, Network Statistics, Event Log, Agent Procedure Log, Remote Control Log, Log Monitoring.
- **Pending Procedures** - Displays and schedules pending procedures for a machine and the procedure history for that machine. Includes the execution date/time, status and user who scheduled the procedure.
  - Click the **Schedule Another Procedure** button to schedule a procedure not yet pending. Once selected and scheduled, the procedure displays at the bottom of the **Pending Procedures** section.
  - Click the **Schedule** button to schedule a selected procedure to run in the future or on recurring basis.
  - Click the **Run Now** button to run a selected procedure once immediately.
  - Click the **Cancel** button to cancel any selected pending procedure.

### Alerts

- Defines alerts for a machine: **Agent Status** (page 222), **Application Status** (page 225), **Get File Changes** (page 227), **Hardware Changes** (page 229), **Low Disk Space** (page 232), **Event Log** (page 234), **LAN Watch** (page 240), **Agent Procedure Failure** (page 243), **Protection Violations** (page 245), **Patch Alert** (page 249), **Backup Alert** (page 252).

### Patch Status

- Displays Missing and Pending Microsoft patches and schedules missing patches. If a machine belongs to a **patch policy** (page 595), missing patches may be further identified as **Denied (Pending Approval)**. The user can manually override the denied patch policy by scheduling the patch.
  - Click the **Schedule** button to schedule a selected missing patch.
  - Click the **Cancel** button to cancel a selected pending patch.
  - Click the **Show History** link to display the history of patches installed on the managed machine.

### Remote Control

## Audit

- Displays the status of remote control sessions for the managed machine: Remote Control, FTP, and Chat. The VSA user can set the remote control package to use during a remote control session.

## Documents

- Lists documents uploaded to the KServer for a managed machine. You can upload additional documents. Provides the same functionality as Audit > [Documents](#) (page 143).

## Users

- [Accounts](#) - Lists all user accounts for the managed machine.
- [Groups](#) - Lists all user groups for the managed machine.
- [Members](#) - Identifies the users belonging to each user group for the managed machine.

## Displaying the Machine Summary Page Using a URL

The following URL displays the [Machine Summary](#) (page 137) web page for a specific machine ID:

`http://...?machName=<MachineID>`

For example:

- `http://demo.kaseya.com?machName=jconners.acme`

---

# System Info

## Audit > System Information

- This page applies to the following products: *On Premises*, *Kaseya Advanced*, *Kaseya Essentials*, *IT Center*, *IT Workbench*
- Similar information is provided using *Info Center > Reports > Inventory* (page 153).

The [System Info](#) page displays all DMI / SMBIOS data collected by the system info [audit](#) (page 587) for a selected machine ID.

## Actions

You can maintain an unlimited number of custom fields of information about managed machines. Custom fields can also be maintained on the Audit > [Machine Summary](#) (page 137) page.

- [New Custom Field](#) - Creates a new custom field.
- [Rename Custom Field](#) - Renames a custom field.
- [Delete Custom Field](#) - Deletes a custom field.

## Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

## Displayed Data

- System Information
  - [Manufacturer](#) - system manufacturer
  - [Product Name](#) - system product name
  - [System Version](#) - system version number
  - [System Serial Number](#) - system serial number
- Network Information

- **IPv4 Address** - IP version 4 address assigned to the machine.
- **IPv6 Address** - IP version 6 address assigned to the machine.
- **Subnet Mask** - Networking subnet assigned to the machine.
- **Default Gateway** - Default gateway assigned to the machine.
- **Connection Gateway** - IP address seen by the KServer when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
- **Country** - The country associated with the Connection Gateway.
- **MAC Address** - MAC address of the LAN card used to communicate with the KServer.
- **DHCP Server** - The IP address of the DHCP server used by this machine.
- **DNS Server 1, 2** - IP address of the DNS servers assigned to the machine.
- **Chassis**
  - **Chassis Manufacturer** - manufacturer of the enclosure
  - **Chassis Type** - enclosure type
  - **Chassis Version** - enclosure version number
  - **Max Memory Slots** - total number of memory module slots available
  - **Chassis Serial Number** - serial number on the enclosure
  - **Chassis Asset Tag** - asset tag number on the enclosure
- **Motherboard**
  - **Motherboard Manufacturer** - motherboard manufacturer
  - **Motherboard Product** - motherboard product ID
  - **Motherboard Version** - motherboard version number
  - **Motherboard Serial Num** - motherboard serial number
  - **External Bus Speed** - motherboard bus speed
- **CPU/RAM Information**
  - **Processor Manufacturer** - processor manufacturer
  - **Processor Family** - processor type installed
  - **Processor Version** - processor version ID
  - **CPU Max Speed** - max processor speed supported
  - **CPU Current Speed** - speed processor is currently running at
  - **CPU** - Processor make and model.
  - **Quantity** - The number of CPUs.
  - **Speed** - Clock speed of the processor.
  - **RAM** - MBytes of RAM on the machine.
  - **Max Memory Size** - maximum memory size the motherboard can hold
  - **Max Memory Slots** - Total number of memory module slots available.
- **Custom Fields** - Displays custom fields and their values.
- **On Board Devices** - Lists motherboard based devices (like video or ethernet).
- **Port Connectors** - Lists all the connections available on the chassis.
- **Memory Devices** - Lists memory modules installed on the motherboard.
- **System Slots** - Displays the status of each available card slot.

---

## Installed Applications

### Audit > Installed Applications

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT

## Audit

### Workbench

- Similar information is provided using [Info Center > Reports > Software - Software Applications Installed](#) (page 174).

The Installed Applications page lists all applications found during the **latest audit** (page 587) for a selected machine ID. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 26). This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).

### Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Application** - The filename of the application.
- **Description** - A brief description of the application as reported in the Properties dialog box of the executable file.
- **Version** - The version number of the application.
- **Manufacturer** - The manufacturer of the application.
- **Product Name** - The product name of the application.
- **Directory Path** - The absolute directory path where the application file is located.
- **File Size** - The size, in kilobytes, of the application file.
- **Last Modified** - The modification date of the application file.

**Note:** You can filter the display of machine IDs on any agent page using the **Contains/Missing application and Version string is > < = N** options in **View Definitions** (page 28).

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

---

## Add/Remove

### Audit > Add/Remove

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*
- Similar information is provided using [Info Center > Reports > Software](#).
- Alerts can be defined using [Monitor > Alerts > Application Changes](#) (page 225).

The **Add/Remove** page displays the programs listed in the **Add or Remove Programs** window of the managed machine. Information shown on this page is collected when a **Latest Audit** (page 134) is performed. Click a machine ID to display data for that selected machine. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 26).

### Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Application Name** - The name of the application.

- **Uninstall String** - The uninstall string in the registry used to uninstall this application.

---

## Software Licenses

### Audit > Software Licenses

- This page applies to the following products: *On Premises*, *Kaseya Advanced*, *Kaseya Essentials*, *IT Center*, *IT Workbench*
- Similar information is provided using *Info Center > Reports > Software*.

The **Software Licenses** page displays all software licenses found for a selected machine ID. The list of machine IDs displayed depends on the **Machine ID / Group ID filter** (page 26) and machine groups the user is authorized to see using *System > User Security > Scopes* (page 404).

Information shown on this page is collected when a **Latest Audit** (page 134) is performed. Each vendor stores an application's license key differently so all application software licenses may not be collected.

### Duplicate License Keys

Duplicate license keys found on more than one machine **display in red text**. Clicking the number link next to the title of a duplicate license lists the machine IDs using the duplicate license.

### Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Publisher** - The software publisher of the application (e.g. Microsoft).
- **Title** - The name of the application.
- **Product Key** - The product key used to activate the application during installation.
- **License** - The license code associated with the application.
- **Version** - The version of the application.
- **Date** - The version release date.

---

## Documents

### Audit > Documents

- This page applies to the following product: *On Premises*
- This function can also be accessed using the *Documents* tab of the *Live Connect* (page 380) > *Agent Data* page and the *Documents* tab of the *Machine Summary* (page 137) page.

The **Documents** page stores files associated with a machine ID. For example, you can upload scanned copies of purchase receipts, contract information, and configuration notes specific to a machine ID.

Uploaded documents are stored in the User Profiles directory of the KServer. For example:

C:\Kaseya\UserProfiles\368905064566500\Docs.

**Note:** Documents are not included in the backup of the KServer database using *System > Configure* (page 412). A separate backup of KServer files and directories should be performed as well.

### To Store a Document

1. Click a machine.group ID link. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 26). Documents previously stored on the KServer for this machine ID display or else *No files found* displays.

## Audit

2. Click **Browse** to locate a file on your local computer or LAN.
3. Click **Upload** to upload the file to the KServer.

The added **Filename** displays, along with its file **Size** and the date/time of the **Last Upload**.

## New Folder

Optionally click the **New Folder** icon and link to create a new folder to store documents in for the selected managed machine.

## Edit

You can click a **Filename** link or edit icon  to display a file or run the file, depending on the application the filename extension is associated with on your local machine.

## Delete

Click the delete icon  to delete a stored document or folder from the KServer.

## Chapter 6

# Info Center

### In This Chapter

Inbox	147
Schedule	147
Reports	149
Reports Sets	177
Customize	180
View Dashboard	180
Layout Dashboard	181

**About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Inbox

## Info Center > Inbox

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Inbox** displays all inbound messages sent to you by other VSA users or by system events. System events include:

- **Reporting** - Reports, Report Sets and Scheduled Reports can all generate an inbox message when a report is generated, if a user is specified as a message recipient.
- **Service Desk** - Service Desk procedures can specify the sending of a message to one or more users. Service Desk generated messages are formatted using Service Desk > Message Templates.

**Note:** Inbox messages are not archived.

## To / CC

Click the   icons to select one or more VSA users to send a message to. You can filter the list of users to select from.

## Editing

You can create a new message or forward an existing message. Use the following toolbar buttons to add special formatting to the text:



-  - Hyperlink selected text. You may need to reset links copied and pasted from another source.
-  or  - Expand or contract the edit pane.
-  - Copy selected text from Microsoft Word and paste into text pane.
-  - Insert a table.
-  - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
-  - Indent text.
-  - Outdent text.
-  - Set selected text to subscript.
-  - Set selected text to superscript.
-  - Remove formatting of selected text.
-  - Insert special characters and symbols.

---

# Schedule

## Info Center > Reporting > Scheduled

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Scheduled** reports page represents your personal list of all *published* reports and report sets you are authorized to view. If your Info Center > **Inbox** (page 147) messages and emails have been deleted, you can always locate a published report you are a recipient of using this page.

- **Displaying Reports** - You can click the  icon next to the name of the report  or report set  to display a **Selected Item History** dialog that contains the publishing history for that report. Click the

publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog.

- **Column Options** - This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).

The following action buttons are provided.

- **Reschedule** - Displays the **Schedule** tab of the **Reschedule Selected Item** dialog. Use this tab to reschedule the publishing of a selected report or report set.
- **Recipients** - Displays the **Distribution** tab of the **Reschedule Selected Item** dialog. Use this tab to change the recipients for a selected report or report set you are rescheduling.
- **Delete Schedule** - Permanently deletes a selected published report or report set. This only deletes the record of the report in **Schedule** for your VSA logon. It does *not* delete the report for any other user.
- **History** - Displays a **Selected Item History** dialog, providing a history of all published instances of the report or report set you have received. Click the publishing date of the report or report set you want to see, then click the hyperlink of a report at the bottom of the dialog.
- **Refresh** - Refreshes the page.

### Rescheduling Selected Item

The **Rescheduling Selected Item** dialog displays the following tabs. *These options apply only to this specific run or scheduling of the report. The report definition remains unchanged.*

- **Schedule** - Schedule the report or report set to run once or periodically. Each type of recurrence—Once, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Clicking the **Submit** button re-publishes the report or report set using the settings currently selected on all four tabs.*
- **Filters** - Filter the selection of data included in the report or report set by organization, machine group, machine ID or view. For some reports or report sets a department filter and service desk filter is available.

**Note:** Filtering by organization or machine group is mandatory for most types of reports and report sets. You can publish reports and report sets across multiple organizations by selecting a **View Definition** (page 28).

- **Distribution** - Select recipients of the report or report set. By default the person running or scheduling the report or report set is selected as an Info Center > **Inbox** (page 147) message recipient. Selected users can be sent an **Inbox** user message or an email. Visibility of users is limited by the scope you are using.
- **General** - Change the report output for reports only. Change the message used to notify users when the report or report set is run. Tokens can be included in report and report set email messages, in both the subject line and the body of the message.
  - <gr> - machine group
  - <id> - machine id
  - <rt> - report name

### Viewing Published Reports and Report Sets

Recipients of reports and report sets can view published reports in these locations:

- In the **Schedule** tab of **Reports** (page 149) and **Reports Sets** (page 177) and in **Scheduled** (page 147), click the  icon next to the name of the report  or report set  to display a dialog box that contains one or more hyperlinks to published reports.

**Note:** Master users can see all scheduled reports. Since scheduled reports contain information about organizations, machine groups, machines, departments, staff and service desks, non-master users can only see scheduled reports created using the same scope they are currently using. To distribute scheduled reports to users outside of the scope you are using, specify them as recipients.

- If published to a recipient's Info Center > **Inbox**, click links embedded in the **Inbox** message.
- If published to a recipient's email address, open the published reports as email attachments.

---

## Reports

### Info Center > Reporting > Reports

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

**Virtual System Administrator™** provides comprehensive reporting for all applications. **Reports** (page 149) can be customized, using report parameters, and filtered by organization, machine group, machine ID or view definition. You can output reports to PDF, HTML, or Excel document and brand reports with your own logo. Reports can be scheduled to run automatically and on a recurring basis. They can be private or shared, distributed to the **Inbox** (page 147) of VSA users or to email recipients. An optional "requires approval" step is provided, just prior to distribution. Reports can also be bundled into **Report Sets** (page 177), enabling you to schedule a standard batch of reports. Your own **Scheduled** (page 147) reports list shows you every report you have access to, so you can always locate any pending report you've created and schedule or any report you've received.

See the following topics for an overview of working with reports.

- **Report Definitions** (page 149)
- **Report Folder Trees** (page 150)
- **Publishing a Report Immediately** (page 151)
- **Scheduling a Report** (page 151)
- **Viewing Published Reports and Reports Set** (page 152)

## Report Definitions

### Report Definitions

A published report is based on a **report definition**. Report definitions contain all the settings that determine the content, layout and file format of the report.

### Report Templates

The first step to creating a report definition is to select a **report template** to base your new report definition on. Click **New Report**.

Report templates determine the basic content of the report and provide default settings for most of the options available in a report definition. Report templates are classified by **report template category**. For example, the report template category `Audit` offers the following kinds of report templates:

- Aggregate Table
- Disk Utilization
- Inventory
- Machine Changes
- Machine Summary
- Network Statistics

Select a category and template, then click **Create**.

## Creating a New Report Definition or Editing an Existing Report Definition

The following tabs are available in both new report definitions and existing report definitions. You can set options in any of the following tabs. *These become the default settings you see when a report definition is run or scheduled.*

- **General** - Sets the report name, report output, and message used to notify users when the report is run.
  - Check the **Suppress Header/Footer** checkbox to suppress adding headers and footers to reports. Reports are generated with page headers and footers by default.
  - Check the **Report Needs Approval Before Distribution** checkbox to require a published report be approved before distribution to recipients.
  - Output to PDF, HTML or Excel. Excel spreadsheet output cannot exceed 65536 rows of data.
- **Report Parameters** - Sets parameters that are specific to the report content. For example, a **Disk Utilization** report provides a parameter just for this type of report called **Show Bar Chart with Percent of Disk Space Used**.

**Note:** By default, VSA report headers display the image specified by the **System > Site Customization > Site Header** (page 429). Changing the value in the **System > Configure > Change URL... (page 418) > Logo** field overrides this default, changing the URL *for report headers only*. Changing the URL in the **Change URL... > Logo** field does not affect the display of the Site Header image.

## Report Folder Trees

Report definitions are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

### Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

### When a Folder is Selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

**Note:** See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 119) topic.

- **New Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **Take Ownership - Takes ownership** (page 119) of a folder you do not own. This option only displays for **master role users** (page 600).
- **New Report** - Opens the report editor to create a new report definition in the selected folder of the folder tree.

### When a Report Definition is Selected

- **New Report** - Opens the report editor to create a new report definition in the selected folder of the folder tree.
- **Edit Report** - Edits the selected report definition.
- **Delete Report** - Deletes the selected report definition.
- **Copy Report** - Copies the selected report definition.
- **Run Now** - Publishes a report based on the selected report definition immediately.
- **Schedule Report** - Schedules publishing of a report based on a selected report definition.

## Publishing a Report Immediately

Select a report in one of the **report folder trees** (page 150), then click **Run Now** to publish the report immediately. A **Data Filter** dialog box opens. "Run Now" filtering defaults from the machine ID / group ID filter. Optionally filter the selection of data included in the report by organization, machine group, machine ID or view. You can publish reports across multiple organizations by selecting a **View Definition** (page 28). For some reports a department filter and service desk filter is available. **Run Now** reports are *not* added to the scheduled list of published reports.

## Scheduling a Report

Select a report in one of the **report folder trees** (page 150), then click **Schedule Report** to display a **Schedule Report** dialog. Use the dialog to schedule publication of the report in the future, once or on a recurring basis. You can set options in any of the following tabs. *These options apply only to this specific run or scheduling of the report. The report definition remains unchanged.*

- **Schedule** - Schedule the report to run once or periodically. Each type of recurrence—Once, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Clicking the **Submit** button publishes the report using the settings currently selected on all four tabs.*
- **Filters** - Optionally filter the selection of data included in the report by organization, machine group, machine ID or view. For some reports a department filter and service desk filter is available.
- **Distribution** - Select recipients of the report. By default the person running or scheduling the report is selected as an Info Center > **Inbox** (page 147) message recipient. Selected users can be sent an **Inbox** user message or an email. Visibility of users is limited by the scope you are using.
- **General** - Change the report output or message used to notify users when the report is run. Tokens can be included in report email messages, in both the subject line and the body of the message.
  - <gr> - machine group
  - <id> - machine id
  - <rt> - report name
  - <embed> - In the message body only, you can embed an HTML report at the specified location.

Once a *scheduled* report begins publishing the following status icons display in the right hand pane.

-  Pending
-  Completed and Approval Required - Click the  icon to view the completed report, then approve or reject it.
-  Completed and Rejected - Click the  icon to view the completed and rejected report. You can subsequently approve it.
-  Completed and Distributed - Click the  icon next to the name of the report to display a **Selected Item History** dialog that contains the publishing history for that report. Click the publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog.
-  Error - The report failed to publish.

The right hand pane of a *scheduled* report provides several columns of information for each time a report is published.

- **Column Options** - This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).
- **Recurring Schedule Columns** - The **Recurrence, Last Ran** and **Next Run** columns describe how often a report is published, when it last ran and when it will run next. The **Recurrence Pattern** and **Ending On** columns describe details of a recurring report.
- **Visibility of Scheduled Reports** - Visibility of rows in the schedule table is limited by the scope you are using. Your selected **view definition** (page 600) has no effect. It does not matter whether you were designated a recipient of the report. Recipients can access the completed report in their **Inbox** (page 147).

The following action buttons are provided for *scheduled* reports.

- **Reschedule** - Displays the **Schedule** tab of the **Reschedule Selected Item** dialog. Use this tab to reschedule the publishing of a selected report. *These options are the same as when you originally schedule a report.*
- **Recipients** - Displays the **Distribution** tab of the **Reschedule Selected Item** dialog. Use this tab to change the recipients for a selected report you are rescheduling. *These options are the same as when you originally schedule a report.*
- **Delete Schedule** - Permanently deletes a selected published report. This only deletes the record of the report in **Schedule** (page 147) for your VSA logon. It does *not* delete the report for any other user.
- **History** - Displays a **Selected Item History** dialog, providing a history of all published instances of the report you have received. Click the publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog.
- **Refresh** - Refreshes the page.

## Viewing Published Reports and Reports Set

Recipients of reports and report sets can view published reports in these locations:

- In the **Schedule** tab of **Reports** (page 149) and **Reports Sets** (page 177) and in **Scheduled** (page 147), click the  icon next to the name of the report  or report set  to display a dialog box that contains one or more hyperlinks to published reports.

**Note:** Master users can see all scheduled reports. Since scheduled reports contain information about organizations, machine groups, machines, departments, staff and service desks, non-master users can only see scheduled reports created using the same scope they are currently using. To distribute scheduled reports to users outside of the scope you are using, specify them as recipients.

- If published to a recipient's Info Center > **Inbox**, click links embedded in the **Inbox** message.
- If published to a recipient's email address, open the published reports as email attachments.

## Antivirus - Antivirus Installation Statistics

Info Center > Reports > Antivirus

- Displays only if the **Antivirus** add-on module is installed.

The **Antivirus Installation Statistics** report definition generates reports for the following types of **Antivirus** data maintained by the VSA.

- **Show Summary Table** - Displays the number of machines installed with **Antivirus** per machine group. Installation details include the install date and version installed, per machine in each machine group.
- **Show Installation Month Bar Chart** - Displays a count of the number of machines installed with **Antivirus**, per month.

## Anti-Malware - Anti-Malware Installation Statistics

Info Center > Reports > Anti-Malware

- Displays only if the [Anti-Malware](#) add-on module is installed.

The [Anti-Malware Installation Statistics](#) report definition generates reports for the following types of [Anti-Malware](#) data maintained by the VSA.

- [Show Summary Table](#) - Displays the number of machines installed with [Anti-Malware](#) per machine group. Installation details include the install date and version installed, per machine in each machine group.
- [Show Installation Month Bar Chart](#) - Displays a count of the number of machines installed with [Anti-Malware](#), per month.

## Audit - Aggregate Table

Info Center > Reports > Audit - Aggregate Table

The [Aggregate Table](#) report definition generates a tabular report mixing any data collected by the VSA. Each report generates a single table with a row for each machine and a column for each piece of data specified.

### Adding and Removing Items

To add items, select items in the left hand list, then click the right arrow  button. To remove items, click items in the right hand list, then click the left arrow  button. To change the order items are listed, click an item in the right hand list, then click the up arrow  or down arrow .

### Advanced Filter

Click the [Advanced Filter](#) (*page 30*) tab to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

## Audit - Disk Utilization

Info Center > Reports > Audit - Disk Utilization

The [Disk Utilization](#) report definition generates a graphical report representing the free space, used space and total space on each disk drive.

Three types of reports are available:

- [Show Bar Chart with Percent of Disk Space Used](#)
- [Show Bar Chart with Disk Space Used, Free Space, and Total Disk Size](#)
- [Show Table with Disk Space Used, Free Space, and Total Disk Size](#)

## Audit - Inventory

Info Center > Reports > Audit - Inventory

- Similar information is provided using [Audit > System Information](#) (*page 140*).

The [Inventory](#) report definition generates a report listing all unique items collected during an audit and identifies the machines containing that item.

### Filtering

Filter fields restrict the items listed in the inventory report to only those items matching the filter. For example, If you run an Inventory report on the [Motherboard Manufacturer](#) field and set the filter to \*Intel\* you will only see items manufactured by Intel, or Intel Corp, or any other variation in the report.

## PCI & Disk HW Inventory Reports

The **PCI & Disk HW** option displays additional fields for filtering the data in the report.

- [Hardware Type](#)
- [Description Notes Filter](#)
- [Product Filter](#)
- [Vendor Filter](#)

## Audit - Machine Changes

[Info Center](#) > [Reports](#) > [Audit - Machine Changes](#)

- Similar information is provided using [Audit > System Information \(page 131\)](#), and [Installed Applications \(page 141\)](#)

The **Machine Changes** report definition generates a differences report between each machine's latest audit and its own baseline *or* compares it to the baseline audit or latest audit from a selected machine. Machine changes examined include CPU, RAM, disk space and applications installed.

Configure your report using the following options:

- **Compare with Machine's own Baseline Audit** - Displays all machine changes found on each machine by comparing the information from the latest audit against the information from the baseline audit.
- **Compare to selected Machine ID** - Displays all machine changes found on each machine by comparing the information from the latest audit against the audit from a *selected machine ID*. Use this function to identify differences in a group of machines when compared against the standard for the group.
- **Use Baseline Audit** - Enabled if **Compare to selected machine ID** is selected. If checked, the selected machine ID's baseline audit is used for comparison instead of the selected machine ID's latest audit.

## Audit - Machine Summary

[Info Center](#) > [Reports](#) > [Audit - Machine Summary](#)

- Similar information is provided using [Audit > Machine Summary \(page 137\)](#) and [Live Connect \(page 380\)](#).

The **Machine Summary** report definition generates a detailed report for each machine ID matching the **machine ID / group ID filter** ([page 592](#)). Use the **Machine Summary** report to generate comprehensive reports for individual machines. Separate "add and remove" selection windows are provided for system data and application data to include in the **Machine Summary** report.

### Machine Summary Sections

The **Machine Summary** report can include the following sections:

- **Add/Remove Programs** - Lists programs in the Add/Remove list of a managed machine.
- **Agent Control/Check-In** - Displays information on baseline and latest audits, last check-in times, quick check-in periods, primary and secondary server and port information.
- **Applications** - Lists applications installed on the managed machine. The list of applications can be filtered by clicking the **App Filter** button.
- **Apps Added Since Baseline** - All new applications detected by **Latest Audit** ([page 134](#)) that have appeared on the machine since the **Baseline Audit** ([page 134](#)) was run.
- **Apps Removed Since Baseline** - All applications that were present when the **Baseline Audit** ([page 134](#)) was ran but are missing when **Latest Audit** ([page 134](#)) last ran.
- **Computer/Network** - Displays the managed machine Windows network name, operating system, CPU, RAM, IP address, gateway, DNS/DHCP server, and WINS server information.
- **Distribute Files** - List files being distributed to the managed machine by the KServer.
- **File Access** - Lists protected files.
- **License Codes** - Lists license codes installed on the managed machine.

- **Logical Disk** - Lists the logical volumes on the managed machines, including removable, fixed, and CD-ROM drives.
- **Miscellaneous** - Lists miscellaneous agent settings, such as WinVNC and user logs status.
- **Network Access** - Lists applications that have restricted network access.
- **PCI Devices** - Lists installed PCI devices on the managed machine.
- **Pending Procedures** - Lists scheduled procedures on the managed machine.
- **Physical Disk** - Lists physical disk information for the managed machine, such as hard disks, DVD, and CD-ROM drives.
- **Printers** - Lists the printers found by the audit for this machine.
- **Recurring Procedures** - Lists procedures that are executed on a scheduled basis on the managed machine.
- **System Info** - All items collected by the **System Info** (page 140) function in the **Audit** module. Click the **Sys Info** button to make additional System Information selections.
- **User Profile** - Lists out user contact information associated with this machine ID.

### Adding and Removing Items

To add items, select items in the left hand list, then click the right arrow  button. To remove items, click items in the right hand list, then click the left arrow  button. To change the order items are listed, click an item in the right hand list, then click the up arrow  or down arrow .

### Advanced Filter

Click the **Advanced Filter** (page 30) tab to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed. This option only displays if you select the **System Info** option above.

## Audit - Network Statistics

### Info Center > Reports > Network Statistics

- Info Center > Reports > Logs > **Network Statistics Log** (page 166) identifies all network access activity.
- Related information is provided using System > Statistics (page 423).

The **Network Statistics** report definition generates a report displaying the *top consumers* of TCP/IP-protocol-based network bandwidth on selected machines. Typically this report refers to bandwidth consumption caused by accessing both internal and external *internet* sites, but can include internal LAN traffic that also uses the TCP/IP protocol.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Report Parameters

- **Applications** - Displays a graph outlining each application and corresponding network bandwidth consumption over the specified period.
- **Machines** - Displays a graph outlining the machines selected in the machine ID / group ID filter and corresponding network bandwidth consumption.
- **Display <N> Consumers of Bandwidth** - The number of top consumers of bandwidth included in the report, either applications or machines.

**Note:** This report requires the **Audit > Network Access** (page 87) driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is *disabled* by default.

## Backup > Backup

Info Center > Reports > Backup

- Displays only if the **Backup** add-on module is installed.
- Similar information is provided using **Backup > Backup Status**.

The **Backup** report definition generates a report summarizing data retrieved from the backup logs.

Configure the report using the following options:

- **Show backup logs from the last <N> days** - Specify how many days of backup log entries to include in the report.
- **Show backup log summary data** - If checked, includes a summary table totaling types of backup events for the last N number of days for volumes and folders.
- **Show backup log status by machine and event** - List the backup log information collected in the last N days for each machine.
  - **Backup type filter** - Volume Backups OR Folder Backups.
  - **Result filter** - <All Results>, Success, Failure, Warning, Informational
- **Ignore machines without data** - If checked, only displays machine IDs that have data matching the other filter parameters.

## Desktop Policy - Desktop Policy

Info Center > Reports > Desktop Policy > Desktop Policy

- Displays only if the **Desktop Policy** add-on module is installed.
- Similar information is provided using **Desktop Policy and Migration > Status**.

The **Desktop Policy** page generates reports for the following types of **Desktop Policy** data maintained by the VSA.

Select the subtopics to include in the **Desktop Policy** report:

- **Include User Type** - List all user groups that each user on the machine is a member of.
- **Include Mapped Drives** - List the drive mappings for each user.
- **Include Printers** - List printer mappings for each user.
- **Include Share points** - List all the directory shares for the machine.
- **Include machines with no data** - Show entries in the report for all machines, including those that have not had **Desktop Policy** information collected.

## Desktop Policy - Power Savings

Info Center > Reports > Power Savings

- Displays only if the **Desktop Policy** add-on module is installed.

The **Power Savings** page generates a report that shows an estimate of how much money can be saved, or has been saved, using a particular power policy. An independent power audit is scheduled as part of the standard audit and collects power settings from all managed machines *including those without the Desktop Policy client installed*.

### Comparison Settings

A power audit is performed on a machine whenever a power policy is applied to the machine and is also performed by the **latest audit** (page 587), typically on a daily basis.

- **Compare machine baseline audit information with:**
  - **Compare With** - Select a defined power policy to see how much you can save by switching over to the selected power policy.
  - **Include All Machines** - If checked, includes the independent power audit results for all Windows 2003 and Windows XP machines without **Desktop Policy** installed along with the results from machines with **Desktop Policy** installed. Checked by default. Does not include Windows 2000, Vista, or 7 machines.
- **Compare most recent power audit data with:**
  - **Compare With - Baseline Power Policy** - Shows power savings by comparing the baseline power policy to the latest audit for each machine. The baseline power policy represents what was in place before **Desktop Policy** was installed on the machine.
  - **Compare With - Last Deployed Power Policy** - Shows power savings by comparing the last deployed power policy to the latest audit for each machine. This value should be the same as the most recent power audit data, unless some of the users have changed their settings since the last time a power policy was applied.
- **Report Period** - Enter the reporting period for the report: Year, Month, From Baseline Collection Time.

### Set Report Values

Set the values that the power savings estimate is based on or leave them set to their default values.

- **Average PC Watts** - Enter the number of watts an average PC in the system uses.
- **Average Monitor Watts** - Enter the number of watts an average monitor in the system uses.
- **Cost of kilowatt-hour (kWh)** - Enter the cost per kilowatt-hour (kWh).
- **Currency Symbol** - Enter the currency symbol associated with the cost entered in the **Cost of kilowatt-hour (kWh)** field. This currency symbol displays in the report.

### Advanced Settings

Make changes to the following advanced settings or leave them set to their default values:

- **PC Watts When Stand By** - Enter the number of watts an average PC uses while it is in standby mode.
- **Workstation Hours Per Day** - Enter the number of hours per day a workstation is in use.
- **Workstation Days Per Week** - Enter the number of days per week the workstation is in use.
- **% of Machines Powered Down at end of Day** - Enter the number of machines that are physically turned off at the end of the day.
- **Workstation Days Idle Per Year (Holidays, Vacations, etc)** - Enter the number of days per year the average workstation is not in use, in addition to weekends.
- **Select Machine Data Based on:**
  - **Most Savings** - If selected, the calculation uses the single user on a machine that provides the highest estimated power savings, as though no other user ever used that machine. This represents the best possible power savings for that machine.
  - **Average User** - If selected, the calculation uses an average of the estimated power savings of all users on a machine, as though each user was logged on to that machine an equal amount of time. This generates an equal or smaller power savings estimate than the **Most Savings** option.
- **Hard Drive Watts** - Enter the number of watts a hard drive uses.
- **Server Hours Per Day** - Enter the number of hours per day a server is in use.

**Note:** Any OS that has the word `Server` in its name is treated as a server for the purposes of this report.

- **Server Days Per Week** - Enter the number of days per week a server is in use.

- **Include Monitors for Servers** - If checked, the calculation assumes each server has a monitor attached and the power settings for the monitors are included.
- **Show Settings per User** - If checked, the report shows the savings for each user on each machine.

## Executive - Executive Summary

Info Center > Reports > Executive - Executive Summary

The **Executive Summary** report definition generates a summary report of the status of all selected machines. This includes a **network health score** (page 159) representing the overall health of all selected machines as a group.

Configure your report definition using the following parameters:

### Time Selection

- **Summarize Data collected in the last N days** - Number of days back from the current date/time to include in the report.

### Report Parameters - Report Selection

- **Show Client Information** - Displays the number of machines, both servers and workstations, and the names of the primary points of contact for this group.
  - **Contact Person** - Optionally enter a customer contact name, representing the point of contact inside the organization receiving the IT service.
  - **IT Manager** - Optionally enter an IT manager name, representing the person responsible for delivering IT services to the client organization.
- **Show System Activity** - Specify search criteria for counting the number of times certain log events occurred. Examples include the number of times machines were audited and scanned for missing patches. Click **Change Rows...** to fully customize this section.
- **Show Ticket Status** - Displays a summary of ticket counts over the specified number of days. If **Service Desk** is installed and activated, displays tickets count only for **Service Desk** tickets. Additional ticket counts display for the number of tickets in each **Service Desk** Status defined. **Uncategorized Tickets** displays if one or more tickets are not set to any Status.
- **Show Anti-Virus Statistics** - Displays Anti-Virus protection and threats statistics.

**Note:** The **Show Anti-Virus Statistics** section only displays if you have installed the **Antivirus add-on** module.

- **Show Disk Space Used for** - Displays a graph of the percentage free disk space on all selected machines. Restrict this chart to servers only by selecting **Show servers only**.
- **Show Percent Uptime for** - Displays a graph of the percentage machines are up for on all selected machines. Restrict this chart to servers only by selecting **Show servers only**.
- **Show Network Health Score** - Displays individual component scores and an overall health score for all the selected machines as a group. See **Network Health Score** (page 159) for details. Click **Change Score...** to fully customize this section.
- **Show Operating Systems** - Displays a pie chart showing the break down of operating systems in the selected group.
- **Show Patch Status** - Displays a pie chart summarizing the state of missing patches for all selected machines.
- **Show Security** - Lists statistics for untreated security protection threats.

**Note:** The **Show Security** section only displays if you have installed the **Endpoint Security add-on** module.

- **Show Alarm Notifications** - Summarizes alerts issued for the specified number of days. This section breaks the alarm count down by category of alarm.
- **Show License Summary** - Summarizes the OS and MS Office licenses found by audit.

- **Show "How to read" notes at end of report** - Displays standard explanatory notes at end of the report. Click [Edit Notes...](#) to customize these notes.

## System Activity

[Info Center](#) > [Reports](#) > [Executive Summary](#) > [System Activity](#)

The **System Activity** section of the **Executive Summary** (page 158) report gives you a summary view of system activity of selected machines as a group. Each row lists a *count* or *value* of a filtered log item in the *last N number of days*.

- Use the **Status** column in the **Pending Procedures** tab of the **Machine Summary** (page 154) page or **Live Connect** (page 380) to identify search filter phrases to use for a procedure-based row type.

**Note:** You must enter at least an \* in the **Search Filter** field to return any results.

- **Log Monitoring** does not display in **Pending Procedures**. Review **Log Monitoring** in **Agent Logs** in the **Machine Summary** page or **Live Connect** to identify search filter phrases to use.
- **Log Monitoring Custom** refers to the *value* or *count* of a numeric log parsing parameter within the *last N number of days*.

Row Type	Search Item	Search Filter Examples	Count
Alarm Log	<All Alarms> or any specific alert/alarm.	* or *text*	Not applicable.
Script Log	Select a system, private or public agent procedure.	*Success THEN* or *Failed ELSE* or *Success ELSE*	Not applicable.
Backup Log	<All Backup Events> or Volume Backups or Folder Backups	*Backup completed successfully*	Not applicable.
Log Monitoring	Select a <a href="#">Log File Parser</a> (page 293).	*device error*	Not applicable.
Log Monitoring Custom	Select a Log File Parser with a numeric parameter.	EventCode or ErrorCode	Average, Count, Min, Max or Total

## Network Health Score

[Info Center](#) > [Reports](#) > [Executive Summary](#) > [Change Score...](#)

The **Network Health Score** section of the **Executive Summary** (page 158) report gives you a summary view of the health and usability of selected machines as a group. The score is broken into **score types**. Each score type is subdivided into one of five possible **percentage buckets**—typically 100%, 75%, 50%, 25% and 0% if none of the first four percentage buckets apply—based on the count for a specified criteria.

**Score Type Calculation Example:** To keep things simple, an **Executive Summary** report only includes three machines. For a single score type within that report, one machine meets the criteria for the 100% bucket. The other two machines meet the criteria for the 75% bucket.  $(100\% + 75\% + 75\%)/3 = 83\%$  health for that score type. You could assign a weight of 2 to double the weight of this score type compared to all the other score types in the report.

**Weight Calculation Example:** You set one score type to a weight of 2 and seven score types to a weight of 1. The total weight for all 8 score types is 9. The percentage of the score type weighted by 2 is multiplied by 2/9 in the final percentage score calculation. In contrast, the percentages of the other

seven score types weighted by 1 are multiplied only by 1/9 in the final percentage score calculation. The final network health score computes the *weighted average* of all score type percentages and normalizes them to provide the final percentage score. 100% represents perfect.

- In most cases, you can customize the counts used to assign percentage scores.
- Set the weight to 0 to turn off that score type.
- For the **OS Score** type only, the standard percentage buckets of 100%, 75%, 50%, and 25% are overridden by the values you set. Each bucket is associated with a different type of operating system. What you're deciding is how healthy a machine should be considered, based on its operating system. Older operating systems tend to be assigned lower **OS Score** percentages.
- You cannot modify the **Patch Score** criteria.

**Note:** Ticketing is ignored when calculating the overall network health score.

**Patch Score** - This score is calculated using the average number of missing patches on each machine. Each machine is scored based on the number of missing patches as follows:

Fully patched	100%
missing 1-2 patches	75%
missing 3-5 patches	50%
missing > 5 patches	25%
unscanned machines	0%

**OS Score** - Modern operating systems score higher than older operating systems. The overall OS score is an average of each machine's score calculated as follows:

Win7/Vista/2008	100%
XP/2003	100%
2000	75%
Mac OS	100%
All others	0%

**Note:** The OS score weighting can be customized. You can individually weight the OS score given to Win7/Vista/2008, 2003, XP and 2000. Enter the % weights (0 to 100) in the four columns normally used for % score. All legacy OSs are given a zero. If you have a large number of legacy OSs deployed, considered turning off the OS score.

**Disk Score** - Full disk drives can have a severe negative impact on your system. As such disk space used contributes to the overall system score. Disk score is computed as follows:

0% to 65% full	100%
65% to 75% full	75%
75% to 85% full	50%
85% to 95% full	25%
100% full	0%

**Ticket Score** - Past due tickets assigned to machines are scored as follows:

0 past due	100%
1 or 2 past due	75%
3 to 5 past due	50%
6 to 10 past due	25%
more than 10 past due	0%

**Note:** The system does not delete tickets when deleting machine IDs. The ticket summary chart includes tickets matching the machine ID / group ID filter. Because no machine data exists for deleted machine IDs, views are not applied to this table.

**Event Log Score** - Monitored event log alerts represent potential system problems. The number of event log alerts generated by each machine over the specified period of time is scored as follows:

0 alerts	100%
1 to 4 alerts	75%
5 to 10 alerts	50%
11 to 20 alerts	25%
more than 20 alerts	0%

**Backup Score** - Counts days since the backup last ran. The older the backup is, the lower the score.

0 to 3 days since last backup ran	100%
4 to 7 days since last backup ran	75%
8 to 14 days since last backup ran	50%
15 to 30 days since last backup ran	25%
more than 30 days since last backup ran	0%

**Alarm Score** - The fewer alarms generated, the higher the score.

0 to 3 alarms	100%
4 to 9 alarms	75%
10 to 19 alarms	50%
20 or more alarms	25%

**Workstation Uptime Score** - The greater the percentage of time workstations are up, the higher the score.

90	100%
80	75%
70	50%
60	25%

**Server Uptime Score** - The greater the percentage of time servers are up, the higher the score.

99	100%
97	75%
95	50%
90	25%

**Security Score** - Untreated threats represent potential system problems. The number of untreated threats generated by each machine over the specified period of time is scored as follows:

0 untreated threats	100%
1 to 4 untreated threats	75%
5 to 10 untreated threats	50%
11 to 19 untreated threats	25%
more than 20 untreated threats	0%

**Note:** The Security Score only displays if you have separately purchased the Endpoint Security add-on module.

**Antivirus Score** - The Antivirus rating is a composite score weighted as follows for each individual machine:

- **Anti-virus install percentage - 40%** - Is Antivirus installed on the machine?
- **Full scans run during the period - 40%** - Has at least one Antivirus scan run during the period?
- **Active threats - 20%** - Has zero threats been detected during the period?

After each machine Antivirus rating is determined, they are grouped into the following percentage buckets, which can be customized: 100%, 75%, 50%, 25%.

**Note:** The Antivirus Score only displays if you have separately purchased the Antivirus add-on module.

**Anti-Malware Score** - The Anti-Malware rating is a composite score weighted as follows for each individual machine:

- **Anti-virus install percentage - 40%** - Is Anti-Malware installed on the machine?
- **Full scans run during the period - 40%** - Has at least one Anti-Malware scan run during the period?
- **Active threats - 20%** - Has zero threats been detected during the period?

After each machine Anti-Malware rating is determined, they are grouped into the following percentage buckets, which can be customized: 100%, 75%, 50%, 25%.

**Note:** The Anti-Malware Score only displays if you have separately purchased the Anti-Malware add-on module.

**Procedure Score** - Procedures provide a recurring beneficial service to a machine. The more often the procedure runs, the better shape that machine is likely to be in. The longer it has been since the procedure ran, the lower the score. The weighted thresholds for the procedure score count the number of days since the procedure last ran on the machines. The default values provide the following score:

1	0 to 3 days since procedure ran	100%
2	4 to 9 days since procedure ran	75%
3	10 to 19 days since procedure ran	50%
4	20 or more days since procedure ran	25%

**Note:** You must enter at least an \* in the Description Filter field to return any results.

## Logs - Logs

Info Center > Reports > Logs - Logs

The **Logs** report definition provides a single point of access for generating any other type of log report. All parameters for all log reports are provided on the Parameters tab. When specifying a log report, only parameters that support that type of log report apply. Consult the following log topics for the parameter fields that apply.

- **Logs - Agent Log** (page 163)
- **Logs - Configuration Changes** (page 164)
- **Logs - Network Statistics** (page 166)
- **Logs - Event Logs** (page 164)
  - Application Event Log
  - Security Event Log
  - System Event Log
  - All Event Logs
- **Logs - Agent Procedure** (page 163)
- **Logs - Admin Notes** (page 163)

- [Logs - Alarm Log](#) (page 163)
- [Logs - Remote Control](#) (page 166)
- [Logs - KES Log](#) (page 165)

## Logs - Admin Notes

[Info Center](#) > [Reports](#) > [Logs - Admin Notes](#)

The [Admin Notes](#) report definition generates reports of [administrator notes](#) (page 14).

Configure your report definition using the following parameters:

- [Number of days to query log\\*](#) - Number of days back from the current date/time to include in the report.
- [Show entries matching the following description \(use \\* for wildcards\)](#) - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Agent Log

[Info Center](#) > [Reports](#) > [Logs - Agent Log](#)

- [Agent](#) > [Agent Logs](#) (page 34) displays log entries by log type and machine ID.

The Agent Log report definition generates a report of agent log entries by machine ID.

Configure your report definition using the following parameters:

- [Number of days to query log\\*](#) - Number of days back from the current date/time to include in the report.
- [Show entries matching the following description \(use \\* for wildcards\)](#) - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Agent Procedure

[Info Center](#) > [Reports](#) > [Logs - Agent Procedure](#)

- [Agent](#) > [Agent Logs](#) (page 34) displays log entries by log type and machine ID.

The [Agent Procedure](#) report definition generates a report of all system and user-defined agent procedures run on each machine ID, including the agent procedure's success or failure status and the VSA user that scheduled them.

Configure your report definition using the following parameters:

- [Number of days to query log\\*](#) - Number of days back from the current date to include in the report.
- [Agent Procedure Name Filter](#) - Filter entries by agent procedure name.
- [Administrator Filter \(Admin that scheduled the agent procedure\)](#) - Filter by the VSA user who scheduled the agent procedure.
- [Show entries matching the following description \(use \\* for wildcards\)](#) - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Alarm Log

[Info Center](#) > [Reports](#) > [Logs - Alarm Log](#)

- [Agent](#) > [Agent Logs](#) (page 34) displays log entries by log type and machine ID.

The **Alarm Log** report definition generates a report of alarm log entries by machine ID. Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Parameters

- **Choose an alert type to display** - Filters by **alert types** (page 586).
- **Filter on email address alarm was sent to** - Filters by alert email recipient.
- **Alarm subject line filter** - Filters by alert email subject line.
- **Alarm message body filter** - Filters by alert email body text.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Configuration Changes

**Info Center > Reports > Logs - Configuration Changes**

- **Agent > Agent Logs** (page 34) displays log entries by log type and machine ID.

The **Configuration Changes** report definition generates a report of VSA setting changes made to each machine ID.

Configure your report definition using the following parameters:

- **Number of days to query log\*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use \* for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Event Logs

**Info Center > Reports > Logs - Event Logs**

- **Agent > Agent Logs** (page 34) displays log entries by log type and machine ID.

The **Event Logs** report definition generates a report of **event log** (page 589) data collected by Windows by machine ID.

Configure your report definition using the following parameters:

- **Display log entries for last N days(s)** - Number of days back from the current date to include in the report.
- **Choose Event Type** - Filter by event log type.
- **Filter by event set** - Filter by a selected event set. Otherwise all events are reported.
- **Event Categories** - Filter by event category.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Event Logs Frequency

**Info Center > Reports > Logs - Event Logs Frequency**

- **Agent > Agent Logs** (page 34) displays log entries by log type and machine ID.

The **Event Logs Frequency** report definition generates a report of the *most frequent event IDs* in **event log** (page 589) data collected by Windows, by machine ID.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Report Parameters

- **Select the <N> most frequent Event IDs for each machine ID** - Select the number of most frequent event IDs.
- **Choose Event Type** - Filter by event log type.
- **Event Categories** - Filter by event category.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - KES Log

**Info Center > Reports > Logs - KES Log**

- Displays only if the **Security** add-on module is installed.
- **Agent > Agent Logs** (page 34) displays log entries by log type and machine ID.

The KES Log report definition generates a report of Endpoint Security log entries by machine ID.

Configure your report definition using the following parameters:

- **Number of days to query log\*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use \* for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Log Monitoring

**Info Center > Reports > Logs - Log Monitoring**

- **Agent > Agent Logs** (page 34) displays log entries by log type and machine ID.

The **Log Monitoring** report definition generates a report of **Log Monitoring** (page 591) log entries.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Report Parameters

- **Choose Log File Parser** - Filter by log parser definition.
- **Show entries matching the following description** - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.

- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Network Statistics Log

### Info Center > Reports > Logs - Network Statistics Log

- Info Center > Reports > Audit > Network Statistics (page 155) identifies *top consumers* of network bandwidth.
- Related information is provided using System > Statistics (page 423).
- Agent > Agent Logs (page 34) displays log entries by log type and machine ID.

The **Network Statistics Log** report definition generates a report of **network statistics** (page 155), by machine ID.

**Note:** This report requires the Audit > Network Access (page 87) driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is disabled by default.

Configure your report definition using the following parameters:

- **Number of days to query log\*** - Number of days back from the current date to include in the report.
- **Show applications matching the following description (use \* for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Logs - Remote Control

### Info Center > Reports > Logs - Remote Control

- Agent > Agent Logs (page 34) displays log entries by log type and machine ID.

The **Remote Control** report definition generates a report of remote control sessions, by machine ID.

Configure your report definition using the following parameters:

- **Number of days to query log\*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use \* for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

## Monitoring - Monitor 95th Percentile

### Info Center > Reports > Monitoring - Monitor 95th Percentile

The **Monitor 95th Percentile** report definition specifies two dates and calculates the 95th percentile, meaning 95% of the time the value is below what is calculated in the report. Identifies *typical* bandwidth requirements for a machine or a device, just below infrequent "peak usage" events. The report supports SLA and planning calculations.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

## Report Parameters

- **Select the monitor set or SNMP set**
- **Percentile** - Set the percentile to use in the report.
- **Select the counters/MIB objects to add to the report** - Select specific counters in the selected monitor set or specific MIB objects within the selected SNMP set to include in the report.

## Monitoring - Monitor Action Log

[Info Center](#) > [Reports](#) > [Monitoring - Monitor Action Log](#)

The **Monitor Action Log** report definition generates a report of **alarm conditions** (page 585) and the actions taken in response to each alarm condition.

A user can assign monitor sets, SNMP sets, alerts, system checks or log monitoring to machine IDs *without checking the Create Alarm checkbox* and a **Monitor Action Log** entry will still be created. These logs enable a VSA user to review *alarm conditions* that have occurred with or without being specifically notified by the creation of an alarm, email or ticket. You can generate a report using [Info Center](#) > [Reports](#) > [Monitoring](#) > **Monitor Action Log** (page 167).

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Report Parameters

- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Message Filter** - Enter a string to filter alarms by their message text. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Sort by Log Event Date Time** - Ascending, Descending

## Monitoring - Monitor Alarm Summary

[Info Center](#) > [Reports](#) > [Monitoring - Monitor Alarm Summary](#)

- *Review alarm conditions without creating alarms using [Info Center](#) > [Reports](#) > [Monitoring](#) > [Monitor Action Log](#) (page 167).*

The **Monitor Alarm Summary** report definition generates a report of created alarms by machine ID.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Report Parameters

- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Alarm Type** - Alarm, Trending

- **Message Filter** - Enter a string to filter alarms by their message text. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Sort by Log Event Date Time** - *Ascending, Descending*
- **Display Message with Each Alarm** - Include a detailed message generated for each alarm.

## Monitoring - Monitor Configuration

[Info Center](#) > [Reports](#) > [Monitoring - Monitor Configuration](#)

The **Monitor Configuration** report definition generates a report of the configuration details of each monitor set assigned to a machine ID or SNMP set assigned to a device.

Configure your report definition using the following parameters:

- **List Assigned Set Only** - If checked, only displays for selection monitor sets assigned to machine IDs and SNMP sets assigned to devices.
- **Select Sets to be Displayed** - Select sets in the right hand pane and click the > button to move them to the right hand pane.

## Monitoring - Monitor Log

[Info Center](#) > [Reports](#) > [Monitoring - Monitor Log](#)

The **Monitor Log** report definition generates a report of monitor log data for monitor sets and SNMP sets, by machine ID, counter and MIB object.

Configure your report definition using the following parameters:

- **Specify the Number of Log Entries for Each Counter and Machine**
- **Show Counter Log Data**
- **Show Service Log Data**
- **Show Process Log Data**
- **Show SNMP Log Data**

## Monitoring - Monitor Set

[Info Center](#) > [Reports](#) > [Monitoring - Monitor Set](#)

The **Monitor Set** report definition generates a report of the monitor logs for a single monitor set or SNMP set, by machine ID.

Configure your report definition using the following parameters:

- **Select Monitor Set** - Select a single monitor set or SNMP set.
- **Display Last** - Number of periods back from the current date/time to include in the report.

## Monitoring - Monitor Trending

[Info Center](#) > [Reports](#) > [Monitoring - Monitor Trending](#)

The **Monitor Trending** report definition generates a report of the monitor logs for a single monitor set counter or for a single SNMP set MIB object, by machine ID.

Configure your report definition using the following parameters:

- **Select Monitor Set** - Select a single monitor set or SNMP set.
- **Select Counter** - Select a counter in the selected monitor set or a MIB object in the selected SNMP set.
- **Display Last** - Number of periods back from the current date/time to include in the report.

## Monitoring - Uptime History

[Info Center](#) > [Reports](#) > [Monitoring - Uptime History](#)

The **Uptime History** report definition generates a graphical report representing:

- When each managed machine was turned on.
- When each managed machine was connected to the network.
- Any abnormal shut downs.

Hovering the mouse over any segment on the chart presents a tool tip that reads out the exact start and end time of that segment.

Configure your report definition using the following parameters:

- **Display N days of Machine Uptime and Online Time** - Number of days back from the current date to include in the report.
- **Display all times in the local time zone for each agent** - Display events in local machine time.
- **Display all times in the system server time zone** - Display events using KServer time.

## Patch - Patch Management

[Info Center](#) > [Reports](#) > [Patch Management](#)

- Similar information is provided using [Patch Management](#) > [Patch Status \(page 312\)](#), [Machine History \(page 318\)](#), [Machine Update \(page 319\)](#) and [Patch Update \(page 318\)](#).

The **Patch Managements** report definition generates a report that lists the patch state for all selected machine IDs. Reports can be filtered by patch category or knowledge base article number. Reports can include patches denied by patch policy. Reports include links to KB articles.

Configure your report definition using the following parameters:

### Display Options

- **Machine Patch Summary Pie Chart** - Display a pie chart showing the number of machines that are:
  - Fully patched systems
  - Missing 1 or 2 patches
  - Missing 3, 4, or 5 patches
  - Missing more than 5 patches
  - Have never been scanned
- **Machine Patch Summary Table** - Display a machine patch summary table.
- **Missing Patch Occurrence Bar Chart** - Display a bar chart illustrating which patches have the most machines that are missing that patch.
- **Table of Missing Patches** - This is a composite report that shows all patches that are missing from any and all machines in the selected group. This table lists a section for each missing patch showing: patch ID, KB article number, and patch title. If `Show (Include machines missing each patch)` is selected, then the report lists each machine ID missing the patch.
- **Table of Installed Patches** - This is a composite report that shows all patches that are installed on any and all machines in the selected group. This table is basically the opposite of the **Table of Missing Patches** section. This table lists a section for each installed patch showing: patch ID, knowledge base article number, and patch title. If `Show (Include machines missing each patch)` is selected, then the report lists each machine ID with the patch installed.
- **Patch Status for each Machine** - For each machine ID a list of both installed and missing patches are shown. Patches are grouped by application. If `Show (include titles for each patch)` is selected, the titles describing the patches are also displayed.
- **Missing Patches for each machine** - For each machine ID a list only of missing patches are shown. Patches are grouped by application. If `Show (include titles for each patch)` is selected, titles describing the patches are also displayed.

## Info Center

- **Patches installed in the last <N> days** - For each machine ID, a list of patches are displayed that were installed during the last number of days specified in the text box. If `Show (include titles for each patch)` is selected, titles describing the patches are also displayed.

## Filters

- **KB Article Numbers and/or Security Bulletin Numbers** - Enter a comma delimited list of KB Article numbers and/or Security Bulletin numbers to generate a report that only lists patches for these numbers.
- **Standard Filter** - Select a filter **criteria** (page 308) for the patch report.
- **Show patches denied by Patch Approval Policy** – By default, only missing patches that have been approved for installation are included in the report. Check the checkbox to ignore the **Patch Approval Policy** (page 595) and include all patches whether approved or denied.

## Security - Security

### Info Center > Reports > Security

- Displays only if the **Security** add-on module is installed.
- Similar information is provided using **Security > Security Status, View Logs, and View Threats**.

The **Security** report definition generates reports for the following types of security data maintained by the VSA.

### Select security report type

Select the type of security report to generate:

- **Configuration Report**
  - Install Time
  - Installer
  - Version
  - License Expiration
  - Assigned Profile
  - Profile Details
  - Alarm Settings
- **Current Threats Report**
  - Summary
  - Threat Category Summary
  - Current Threats
- **Historical Threats Report**
  - Summary
  - Threat Category Summary
  - Current Threats

## Service Desk - Custom Tickets

### Info Center > Reports > Service Desk - Custom Tickets

- Displays only if the **Service Desk** add-on module is installed.

The **Custom Tickets** report definition generates a report displaying **Service Desk** ticket summary information and ticket details.

Configure your report definition using the following parameters.

## General

- **Service Desk**
- **Notes / Summary / Submitter Filter** - List only tickets or ticket counts containing this string in any note, summary line or submitter information line. Use \* for wildcard.
- **Display all Tickets** - If checked, list all tickets individually.
- **Display Notes with each ticket** - If checked, display notes with each ticket.
- **Hide Hidden Notes** - If checked, hide hidden notes.
- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category Column of Data** - Assignee, Status, Priority, Category, Sub Category.

## Time Range

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

## Columns

Values for all desk definitions are displayed in the drop-down lists. Select multiple items using Ctrl+Click and Shift+Click, unless otherwise noted.

- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

## Filters

- **Assignee Filter** - Only one item can be selected.
- **Status Filter**
- **Priority Filter**
- **Category Filter**
- **SubCategory Filter** - Only displays subcategories for selected categories in the **Category Filter**.

## Service Desk - Service Goals

Info Center > Reports > Service Desk - Service Goals

- Displays only if the Service Desk add-on module is installed.

The **Service Goals** report definition generates a report displaying summary information and ticket details related to meeting **Service Desk** goals.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

### Parameters

- **Include Only Tickets with Goals** - If checked, only tickets with goals are displayed.
- **Select Report-By Type** - Service Goals by Ticket, Ticket Number.

- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

## Service Desk - Service Hours

Info Center > Reports > Service Desk - Service Hours

- Displays only if the [Service Desk](#) add-on module is installed.

The **Service Hours** report definition generates a report displaying summary information and ticket details related to **Service Desk** hours worked.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Parameters

- **Include Only Tickets with Goals** - If checked, only tickets with goals are displayed.
- **Select Report-By Type** - `Service Hours by Ticket`, `Service Hours by Contributor`, `Service Hours by Organization`.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

## Service Desk - Service Times

Info Center > Reports > Service Desk - Service Times

- Displays only if the [Service Desk](#) add-on module is installed.

The **Service Times** report definition generates a 12-month report, starting with a specified month and year, showing how many tickets have been created, closed, resolved, past due within fixed time buckets.

Configure your report definition using the following parameters:

### Parameters

- **Month** - Select a month.
- **Year** - Select a year.
- **Display Tickets Created** - If checked, display tickets created.
- **Display Tickets Closed** - If checked, display tickets closed.
- **Display Tickets Resolved** - If checked, display tickets resolved.
- **Display Tickets Past Due** - If checked, display tickets past due.
- **Display Ticket Service Time Details Tables** - If checked, display tickets detail tables.

## Service Desk - Service Volumes

Info Center > Reports > Service Desk - Service Volumes

- Displays only if the [Service Desk](#) add-on module is installed.

The **Service Volumes** report definition generates a 12-month report, starting with a specified month and year, showing the number of tickets in each month that belong to each possible value in a specified ticket column.

Configure your report definition using the following parameters:

## Parameters

- **Group by** - Select the column to group by.
- **Sort Column Direction** - Ascending, Descending.
- **Month** - Select a month.
- **Year** - Select a year.
- **Display Ticket Volumes Chart** - If checked, display a tickets volumes chart.

## Service Desk - Tickets

Info Center > Reports > Service Desk - Tickets

- Displays only if the [Service Desk](#) add-on module is installed.

The **Tickets** report definition generates a report displaying **Service Desk** ticket summary information and ticket details.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Parameters

- **Notes / Summary / Submitter Filter** - List only tickets or ticket counts containing this string in any note, summary line or submitter information line. Use \* for wildcard.
- **Display all Tickets** - If checked, list all tickets individually.
- **Display Notes with each ticket** - If checked, display notes with each ticket.
- **Hide Hidden Notes** - If checked, hide hidden notes.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.
- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category Column of Data** - Assignee, Status, Priority, Category, Sub Category.

### Column Filters

Values for all desk definitions are displayed in the drop-down lists. Select multiple items using `Ctrl+Click` and `Shift+Click`, unless otherwise noted.

- **Assignee Filter** - Only one item can be selected.
- **Status Filter**
- **Priority Filter**
- **Category Filter**
- **SubCategory Filter** - Only displays subcategories for selected categories in the **Category Filter**.

## Software - Software Applications Changed

Info Center > Reports > Software - Software Applications Changed

- Similar information is provided using [Audit > Add/Remove](#) (page 142).

The **Software Applications Changed** report definition generates a report displaying lists of applications

added to and removed from machine IDs. Uses data collected from the latest audit.

**Note:** This report was called the **Software - Add/Removes Programs** report before the Kaseya 2 release.

Configure your report definition using the following parameters:

- **Add/Remove List Item Filter** - Enter a string to filter items by their name. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **List machine IDs that contain each application** - If checked, then the machine ID of each machine add/remove program is listed.

## Software - Software Applications Installed

[Info Center](#) > [Reports](#) > [Software - Software Applications Installed](#)

- Similar information is provided using [Audit](#) > [Installed Applications](#) (page 141).

The **Software Applications Installed** report definition generates a report displaying each unique application found on all machines. The total number of unique copies of the application are also listed. Uses data collected from the latest audit.

Configure your report definition using the following parameters:

- **Application Filter** - Filters by application name (theApp.exe).
- **Product Name Filter** - Filters by product name string as provided by the software vendor.
- **Description Filter** - Filters by software description string as provided by the software vendor.
- **Manufacturer Filter** - Filters by software vendor name.
- **Version Filter** - Filters by software version number.
- **Show Unregistered Applications** - If checked, includes programs not in the registry. Registered applications place an `App Paths` key in the registry identifying the location of their main executable. Sorting on this value is a good way to separate main applications from all the helper and secondary applications.
- **List machine IDs that contain each application** - If checked, then the machine ID of each machine installed with the program is listed.
- **Display Column(s)** - Application, Product, Description, Manufacturer, Version.
- **Sort By** - Application, Product, Description, Manufacturer, Version.

## Software - Software Licenses

[Info Center](#) > [Reports](#) > [Software - Software Licenses](#)

- Similar information is provided using [Audit](#) > [Software Licenses](#) (page 143).

The **Software Licenses** report definition generates a report listing the number of software licenses found in a group of machines. This report lists the total number of licenses and the number of unique licenses found across all machines. Uses data collected from the latest audit.

Configure your report definition using the following parameters:

- **Show Publisher matching** - Filters by software vendor name.
- **Show Title matching** - Filters by software title.
- **Do Not List Machine IDs** - Machine IDs are not listed.
- **List Machine IDs** - The machine ID of each machine installed with the application is listed.
- **List Machine IDs by License Code** - License codes and product keys installed on each machine are displayed.

## Software - Software Licenses Summary

[Info Center](#) > [Reports](#) > [Software - Software Licenses Summary](#)

- Similar information is provided using [Audit](#) > [Software Licenses](#) (page 143).

The **Software Licenses** report definition generates a table summarizing the licenses on all machines in a group or view. Uses data collected from the latest audit. This report presents four tables of information summarizing the following:

- **Servers** - Lists all server types found and the number of machines running that server OS.
- **Workstations** - Lists all workstation types found and the number of machines running that workstation OS.
- **Microsoft Office Licenses** - Lists the number of machines with each version of Microsoft Office loaded.
- **Other Applications** - Summarizes the number of machines with each application license found that is not contained in the first 3 tables.

Configure your report definition using the following parameters:

- **Show Publisher matching** - Filters by software vendor name.
- **Show Title matching** - Filters by software title.

## Software - Software Operating Systems

[Info Center](#) > [Reports](#) > [Software - Operating Systems](#)

The **Operating Systems** report definition generates a composite view chart of all operating systems found on all machine IDs.

**Note:** Each machine reports its operating system type and version with each check-in. Audit does not have to complete to obtain operating system information. Therefore, the number of operating systems reported by this report may be higher than the number of licenses reported for that operating system if all machines have not completed an audit.

Configure your report definition using the following parameters:

- **Show Pie chart**
- **Show Bar chart**
- **Show Table**

## Ticketing - Customizable Ticketing

[Info Center](#) > [Reports](#) > [Ticketing](#) > [Customizable Ticketing](#)

- Similar information is provided using [Ticketing > View Summary \(page 435\)](#).

The **Customizable Ticketing** report definition generates a report listing all **Ticketing** module tickets assigned to selected organizations, machine groups, machines, departments, or staff records.

Configure your report definition using the following parameters:

### Time Selection

- **Select the Time Range** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

### Parameters

- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category** - Assignee, Status, Category, Priority.
- **Display none** - Do not list individual tickets in the report.
- **Display all tickets** - List all tickets individually.

## Info Center

- **Display all tickets with notes** - List all tickets, include both public and hidden notes.
- **Display all tickets but hide hidden notes** - List all tickets, include public notes but hide hidden notes.

## Filters

- **Notes/Summary/Submitter Field** - Enter a string to filter tickets by their notes or summary line or submitter fields. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Assignee Filter** - Filter tickets by Assignee.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.
- **Status** - Filter tickets by Status
- **Category** - Filter tickets by Category.
- **Priority** - Filter tickets by Priority.
- **Resolution** - Filter tickets by Resolution.
- **(Custom Fields)** - Filter tickets by one or more Custom Fields.

## Columns

Select the tickets columns included in the report. All columns are included by default.

## Ticketing - Ticketing

[Info Center](#) > [Reports](#) > [Ticketing](#) > [Ticketing](#)

- Similar information is provided using [Ticketing](#) > [View Summary](#) (page 435).

The **Ticketing** report definition generates a report listing all **Ticketing** module tickets assigned to selected organizations, machine groups, machines, departments, or staff records.

Configure your report definition using the following parameters:

## Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

## Parameters

- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category** - Assignee, Status, Category, Priority.
- **Notes / Summary / Submitter Filter** - List only tickets or ticket counts containing this string in any note, summary line or submitter information line. Use \* for wildcard.
- **Display none** - Do not list individual tickets in the report.
- **Display all tickets** - List all tickets individually.
- **Display all tickets with notes** - List all tickets, include both public and hidden notes.
- **Display all tickets but hide hidden notes** - List all tickets, include public notes but hide hidden notes.
- **Notes/Summary/Submitter Field** - Enter a string to filter tickets by their notes or summary line or submitter fields. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- Filter tickets by
  - **Assignee**
  - **Status**
  - **Category**

- **Priority**
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

## Time Tracking - Timesheet Summary

[Info Center](#) > [Reports](#) > [Time Tracking](#) > [Timesheet Summary](#)

The **Timesheet Summary** report definition generates a report listing the status of all timesheets for a specified date range.

Configure your report definition using the following parameters.

### Time Selection

- **Custom Start DateTime** - The start date.
- **Custom End DateTime** - The end date.

### Parameters

- **Choose Group Type** - Grouped by `Period` or by `Status`.
- **Staff List** - The staff to include in the report. The list comprises all staff with timesheets that your scope authorizes you to see.

**Note:** For each staff record and time period, a timesheet is only created if at least one time entry is added to the timesheet.

## Time Tracking - Timesheet Entries

[Info Center](#) > [Reports](#) > [Time Tracking](#) > [Timesheet Entries](#)

The **Timesheet Entries** report definition generates a report listing all timesheet entries for a specified date range.

Configure your report definition using the following parameters.

### Time Selection

- **Custom Start DateTime** - The start date.
- **Custom End DateTime** - The end date.

### Parameters

- **Staff List** - The staff to include in the report. The list comprises all staff with timesheets that your scope authorizes you to see.

---

## Reports Sets

[Info Center](#) > [Reporting](#) > [Report Sets](#)

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center*

A **report set** is a *collection* of **report definitions** (*page 149*). You can schedule a *report set definition* just like you would an individual *report definition*. This saves you the trouble of scheduling individual report definitions one at a time.

See the following topics for an overview of working with report sets.

- **Report Set Definitions** (*page 178*)
- **Report Set Folder Trees** (*page 178*)
- **Scheduling a Report Set** (*page 179*)

- [Viewing Published Reports and Reports Set](#) (page 152)

## Report Set Definitions

A **report set** is a *collection* of **report definitions** (page 149). You can schedule a *report set definition* just like you would an individual *report definition*. This saves you the trouble of scheduling individual report definitions one at a time.

### Creating a New Report Set Definition

Click the **New Report Set** button to create a new report set definition. The **New Report Set** dialog displays the following tabs.

#### General

- **General** - Enter the report set name and description.
- **Message** - Enter the default subject line and message used to notify users when the report set is distributed.

#### Reports

- Check the report definitions you want to include in the report set definition.

### Editing an Existing Report Set Definition

1. Click an existing report set definitions in the **report set folder trees** (page 178) in the middle pane.
2. Click the **Edit Report Set** button to edit the report set definition. The **Edit Report Set** dialog displays the same options as the **New Report Set** dialog described above.

### Viewing Report Set Definition Properties

1. Click an existing report set definitions in the **report set folder trees** (page 178) in the middle pane.
2. You can view the configuration of the report set definition in the right hand pane:
  - The **Assigned Reports** section of the **Schedule** tab displays the report definitions included in the report set. You can **Assign** or **Remove** report definitions using this section.
  - The **General** tab displays the default subject line and message used to notify users when the report set is distributed.

## Report Set Folder Trees

Report set definitions are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

#### Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

#### When a Folder is Selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

**Note:** See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 119) topic.

- **New Folder** - Creates a new folder underneath the selected cabinet or folder.

- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **Take Ownership** - **Takes ownership** (page 119) of a folder you do not own. This option only displays for master role users.
- **New Report Set** - Opens the report set editor to create a new report set definition in the selected folder of the folder tree.

#### When a Report Set Definition is Selected

- **New Report Set** - Opens the report set editor to create a new report set definition in the selected folder of the folder tree.
- **Edit Report Set** - Edits the selected report set definition.
- **Delete Report Set** - Deletes the selected report set definition.
- **Schedule Report Set** - Schedules publishing of the selected report set definition.

## Scheduling a Report Set

Click **Schedule Report Set** to schedule the report set to run in the future, once or on a recurring basis. You can set options in any of the following tabs. *A report in a report set uses the parameters and output as configured on the report instance. The filters and distribution are set by the report set.*

- **Schedule Report Set** - Schedule the report set to run once or periodically. Each type of recurrence—Once, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence.
- **Filters** - Optionally filter the selection of data included in the report set by organization, machine group, machine ID or view. For some report sets a department filter and service desk filter are available.

**Note:** All individual report definitions in the report set use the filtering and distribution settings you select when a report set is run or scheduled.

- **Distribution** - Select recipients of the report set. By default the person running or scheduling the report set is selected as an Info Center > **Inbox** (page 147) message recipient. Selected users can be sent an **Inbox** user message or an email. Visibility of users is limited by the scope you are using.
- **General** - Change the message used to notify users when the report set is run. Tokens can be included in report set email messages, in both the subject line and the body of the message.
  - <gr> - machine group
  - <id> - machine id
  - <rt> - report name
  - <embd> - In the message body only, you can embed an HTML report at the specified location.

Once a *scheduled* report set begins publishing the following status icons display in the **Schedule** tab in the right hand pane.

-  Pending
-  Completed and Approval Required - Click the  icon to view the completed report, then approve or reject it.
-  Completed and Rejected - Click the  icon to view the completed and rejected report. You can subsequently approve it.
-  Completed and Distributed - Click the  icon next to the name of the report set to display a **Selected Item History** dialog that contains the publishing history for that report. Click the publishing

date of the report set you want to see, then click the hyperlinks for any of the reports at the bottom of the dialog.

-  Error - The report set failed to publish.

The **Schedule** tab in the right hand pane of a *scheduled* report set provides several columns of information for each time a report set is published.

- **Column Options** - This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).
- **Recurring Schedule Columns** - The **Recurrence, Last Ran** and **Next Run** columns describe how often a report set is published, when it last ran and when it will run next. The **Recurrence Pattern** and **Ending On** columns describe details of a recurring report.
- **Visibility of Scheduled Report Sets** - Visibility of rows in the schedule table is limited by the scope you are using. Your selected **view definition** (page 600) has no effect. It does not matter whether you were designated a recipient of the report set. Recipients can access the completed report set in their **Inbox** (page 147).

The following action buttons are provided for *scheduled* report sets.

- **Reschedule** - Displays the **Schedule** tab of the **Reschedule Selected Item** dialog. Use this tab to reschedule the publishing of a selected report set. *These options are the same as when you originally schedule a report set.*
- **Recipients** - Displays the **Distribution** tab of the **Reschedule Selected Item** dialog. Use this tab to change the recipients for a selected report or report set you are rescheduling. *These options are the same as when you originally schedule a report set.*
- **Delete Schedule** - Permanently deletes a selected published report set. This only deletes the record of the report set in **Schedule** (page 147) for your VSA logon. It does *not* delete the report set for any other user.
- **History** - Displays a **Selected Item History** dialog, providing a history of all published instances of the report set you have received. Click the publishing date of the report set you want to see, then click the hyperlink of a report at the bottom of the dialog.
- **Refresh** - Refreshes the page.

---

## Customize

Info Center > Customize

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Customize** page sets defaults for report definitions. Defaults include:

- **Default Paper Size**
- **Default Distribution**
- **Report Theme**

---

## View Dashboard

Info Center > Dashboard > View Dashboard

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **View Dashboard** page gives you a quick view of the total system's status, highlighting the machine IDs and tasks you need to work on first. The results displayed by the dashboard depend on the **Machine ID / Group ID filter** (page 592). You can manage **tasks** and send **messages** to other users using the dashboard. Customize the dashboard display using InfoCenter > **Layout Dashboard** (page 181).

## Agent Status

Summarizes the online status of all machine IDs matching the current machine ID / group ID filter. Gives you an at-a-glance count of how many machines are **online**, have **users logged into** them, have been offline for **less than 30 days** and offline for **over 30 days** and the **total number of agents** matching the current machine ID / group ID filter.

## Patch Status

Uses a pie chart to highlight machines missing patches and matching the current machine ID / group ID filter. The chart displays with or without applying a patch policy.

- Click the **Use Policy** button to apply the **Patch Policy** (*page 595*) when generating the pie chart.

**Note:** The Patch Policy incurs a significant performance penalty. If you have a lot of machine IDs this pie chart takes a long time to generate when using the patch policy.

- Click the **Hide Policy** button to generate the pie chart without the patch policy. This shows all missing patches including those denied by patch policy.
- Clicking on any pie segment opens a sub window listing all machine IDs that make up that pie segment.

## Operating Systems

Uses a pie chart to shows the mix of operating systems in use, for machines matching the current machine ID / group ID filter. Clicking any pie segment opens a sub window listing all machine IDs that make up that pie segment.

## Tickets

Lists recent tickets issued against the machine IDs matching the current machine ID / group ID filter. Applies to **Ticketing** module tickets only.

## System Status

Identifies the number of current and total VSA users and **Portal Access** (*page 81*) users. Also displays the size of the database, the database size per machine account and the last backup date.

## Tasks

Use this section to create, edit, and monitor tasks you or other users need to perform. A pop up window alerts you when new tasks created for you have been added to your task list. Additional pop ups occur when the task becomes past due. You can have the system remind you of a past due task again, by clicking the **Snooze** button when the task reminder dialog box displays. You can clear all outstanding task notification messages by clicking the **Clear Snooze** button on the System > **Preferences** (*page 391*) page.

## Messages

Use this section to send messages to other VSA users. Other VSA users see the messages as popup windows. Messages you have received are listed in the lower part of this pane.

**Note:** Send messages to machine users using Remote Control > **Send Message** (*page 375*).

---

# Layout Dashboard

Info Center > Dashboard > Layout

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT

### Workbench

The **Layout Dashboard** page displays/hides each section of the **View Dashboard** (*page 180*) page and sets the order they appear, from top to bottom. To display an item, check the box next to the item.

Two items have additional customization control: **Tickets**, and **Messages**. Both display time dependent data. To make it easy to quickly distinguish new item from old items, you can specify different highlight colors from data rows depending on how recently the data item was generated.

### Recommendation

- Highlight the most recent tickets and messages in red. All tickets and messages created in the last N days are **highlighted in red**.
- Highlight the next most recent tickets and messages in yellow. All tickets and messages that are older than the red highlight date but more recent than the number entered are **highlighted in yellow**.
- Disable highlighting by setting the number of days to zero.

## Chapter 7

# Monitor

### In This Chapter

Monitor Overview	185
Alarms	187
Dashboard List	189
Dashboard Settings	197
Alarm Summary	198
Suspend Alarms	199
Live Counter	201
Monitor Lists	202
Update Lists By Scan	203
Monitor Sets	204
SNMP Sets	212
Alerts	219
SNMP Traps Alert	257
Assign Monitoring	261
Monitor Log	267
System Check	269
LAN Watch	272
Assign SNMP	276
SNMP Log	284
Set SNMP Values	286
Set SNMP Type	287
Parser Summary	288
Log Parser	292
Assign Parser Sets	297
Viewing Log Monitoring Entries	302

## **Monitor**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Monitor Overview

## Monitor

The **Monitoring** module in **Virtual System Administrator™** provides five methods of monitoring machines and log files:

- **Alerts** - Monitors events on *agent-installed* machines.
- **Monitor Sets** - Monitors the performance state on *agent-installed* machines.
- **SNMP Sets** - Monitors the performance state on *non-agent-installed devices*.
- **System Check** - Monitors events on *non-agent-installed* machines.
- **Log Monitoring** - Monitors events in *log files*.

You can monitor the health in real time of managed machines and SNMP devices and be notified immediately if any problems arise. When programmable alarms are triggered, **Monitor** executes email notifications, procedures and job ticketing, for such problems and state changes as:

- When any critical server or desktop computer goes off-line.
- When a machine user disables remote control.
- When any software application is added or removed.
- When the hardware configuration changes.
- When the computer is running low on disk space.
- When a specific event or any event log entry is generated.
- When any protection policy violation occurs.
- When any agent procedure fails execution.
- When an unapproved application attempts to access the network.
- When an unapproved application attempts to access a protected file.
- When a new device appears on the local area network.
- When an external log records a specific log entry.

In addition to generating alert notifications when **event log entries** are generated, event log entries collected from your managed machines are stored on the VSA. The event log data is always available, even if the managed machine goes offline or suffers a hard failure. Event log data is presented in a familiar and concise form using the Agent > **Agent Logs** (*page 34*) page, as well as Info Center > Reports > Logs.

**Note:** You can download a **Monitoring Configuration PDF** from the first topic of online user assistance.

**Note:** You can download a **Configuring Log Parsers Step-by-Step PDF** from the first topic of online user assistance.

**Note:** **Kaseya Monitor™ Service** (<http://www.kaseya.com/services/it-services.aspx>) extends monitoring past nine-to-five. By out-tasking systems management and monitoring during off-hours, MSPs can offer customers 24/7/365 "Always-On" monitoring.

---

Function	Description
<a href="#">Dashboard List</a> ( <i>page 189</i> )	Provides multiple monitoring views.
<a href="#">Dashboard Settings</a> ( <i>page 197</i> )	Users can customize the Dashboard List page.
<a href="#">Alarm Summary</a> ( <i>page 198</i> )	Lists alarms for monitored machines.
<a href="#">Suspend Alarms</a> ( <i>page 199</i> )	Suspends alarm notifications for specific machine IDs.
<a href="#">Live Counter</a> ( <i>page 201</i> )	Displays live performance counter data for a selected

## Monitor

	machine ID.
<b>Monitor Lists</b> (page 202)	Configures the monitor list objects for monitoring.
<b>Update Lists By Scan</b> (page 203)	Scans machines for monitor counters and services.
<b>Monitor Sets</b> (page 204)	Configures monitor sets.
<b>SNMP Sets</b> (page 212)	Configures SNMP monitor sets.
<b>Add SNMP Object</b> (page 217)	Manages SNMP MIB objects.
<b>Alerts</b> (page 219)	Configures monitor alerts for machines.
<b>SNMP Traps Alert</b> (page 257)	Configures alerts for SNMP Trap event log entries created on selected managed machines.
<b>Assign Monitoring</b> (page 261)	Assigns, removes and manages alarms of monitor sets on machines.
<b>Monitor Log</b> (page 267)	Views monitor log data in chart and table format.
<b>System Check</b> (page 269)	Assigns, removes and manages alarms for system checks on machines.
<b>LAN Watch</b> (page 272)	Scans network range for specific SNMP enabled devices.
<b>Assign SNMP</b> (page 276)	Assigns, removes and manages alarms of SNMP monitor sets on devices.
<b>SNMP Log</b> (page 284)	Views SNMP log data in chart and table format.
<b>Set SNMP Values</b> (page 286)	Sets SNMP values on the specified device.
<b>Set SNMP Type</b> (page 287)	Assigns SNMP types to SNMP devices.
<b>Parser Summary</b> (page 288)	Defines alerts for parser sets and copy parser set assignments to multiple machine IDs.
<b>Log Parser</b> (page 292)	Defines log parsers and assigns them to machine IDs.
<b>Assign Parser Sets</b> (page 297)	Creates and assigns parsers sets to machine IDs and creates alerts on parser set assignments.

---

# Alarms

The same alarm management concepts and guidelines apply to all methods of monitoring.

## Alarm Conditions

An alarm condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

## Alarms

In graphical displays throughout the VSA, when an **alarm condition** (page 585) exists, the VSA displays, by default, a red traffic light  icon. If no alarm condition exists, a green traffic light icon  displays. These icons can be customized.

Alarms, and **other types of responses** (page 586), are enabled using the following pages:

- Agent > **LAN Watch** (page 56)
- Backup > Backup Alerts
- Monitor > **Alerts** (page 219)
- Monitor > **Assign Monitoring** (page 261)
- Monitor > **SNMP Traps Alert** (page 257)
- Monitor > **Assign SNMP** (page 276)
- Monitor > **System Checks** (page 269)
- Monitor > **Parser Summary** (page 288)
- Monitor > **Assign Parser Sets** (page 297)
- Patch Management > **Patch Alerts** (page 342)
- Remote Control > Offsite Alerts
- Security > Apply Alarm Sets

## Five Methods of Monitoring

Each of the five methods of monitoring in Virtual System Administrator™ is either event-based or state-based.

- Event-based
  - **Alerts** - monitors events on *agent-installed* machines
  - **System Check** - monitors events on *non-agent-installed* machines
  - **Log Monitoring** - monitors events in *log files*
- State-based
  - **Monitor Sets** - monitors the performance state on *agent-installed* machines
  - **SNMP Sets** - monitors the performance state on *non-agent-installed devices*

## Event-Based Alarms

**Alerts** (page 219), **System Check** (page 269) and **Log Monitoring** (page 292) represent **event-based alarms** that occur perhaps once. For example a backup may fail. There is no transition out of the condition, it just happens. Since there is no state, the red alarm in a dashlet never transitions back to green until you close the alarm in the alarm log. Typically event-based alarms are easier to configure, since the possibilities are reduced to whether one or more of the events happened or did not happen within a specified time period.

## State-Based Alarms

**Monitor set** (page 204) counters, services, and processes and **SNMP set** (page 212) objects are either currently within their expected state range or outside of it and display as red or green alarm icons *dynamically*. These are known as **state-based alarms**.

## Monitor

- If an alarm state currently exists, monitor dashlets (page 189) show red alarms.
- If an alarm state does not currently exist, monitor dashlets show green alarms.

For monitor sets and SNMP sets, the criteria for an alarm condition can be tailored using [Auto Learn](#) (page 266) and [Individualized](#) (page 261) sets. Alarms for monitor sets and SNMP sets can be *dismissed* using the [Network Status](#) (page 193) dashlet. Typically state-based alarms require more thought to configure than event-based alarms, because the intent is to measure the level of performance rather than outright failure.

### Reviewing Created Alarms

All alarm conditions that have the [Create Alarm](#) checkbox checked—both state-based alarms and event-based alarms—are recorded in the [alarm log](#). An alarm listed in the alarm log does not represent the *current state* of a machine or device, rather it is a *record* of an alarm that has occurred *in the past*. An alarm log record remains `Open` until you close it. Alarms can also be deleted from the alarm log. Note that a state-based alarm, like a monitor set or SNMP set, can trigger an alarm state that changes to red and then changes back to green. This same state-based alarm, if the [Create Alarm](#) checkbox is checked, can also generate an alarm *record* that remains `Open` until you close it.

Created alarms can be reviewed, `Closed` or [Deleted...](#) using:

- Monitor > [Alarm Summary](#) (page 198)
- Monitor > Dashboard List > any [Alarm Summary Window](#) (page 192) within a dashlet
- Agent > Agent Logs > [Alarm Log](#) (page 34)
- [Live Connect](#) (page 380) > Agent Data > Agent Logs > Alarm Log

Created alarms can also be reviewed using:

- Monitor > Dashboard List > [Alarm List](#) (page 191)
- Monitor > Dashboard List > [Alarm Network Status](#) (page 191)
- Monitor > Dashboard List > [Alarm Rotator](#) (page 193)
- Monitor > Dashboard List > [Alarm Ticker](#) (page 193)
- Monitor > Dashboard List > [Group Alarm Status](#) (page 193)
- Monitor > Dashboard List > [Monitor Set Status](#) (page 194)
- Monitor > Dashboard List > [Monitor Status](#) (page 196)
- Monitor > Dashboard List > [Top N - Monitor Alarm Count](#) (page 196)
- Monitor > Dashboard List > [KES Status](#) (page 197)
- Monitor > Dashboard List > [KES Threats](#) (page 197)
- Info Center > Reports > Monitoring > Logs > Alarm Log
- Info Center > Reports > Monitoring > Monitor Action Log

### Reviewing Alarm Conditions with or without Creating Alarms

A user can assign monitor sets, SNMP sets, alerts, system checks or log monitoring to machine IDs *without checking the Create Alarm checkbox* and a [Monitor Action Log](#) entry will still be created. These logs enable a VSA user to review *alarm conditions* that have occurred with or without being specifically notified by the creation of an alarm, email or ticket. You can generate a report using Info Center > Reports > Monitoring > [Monitor Action Log](#) (page 167).

### Reviewing Performance with or without Creating Alarms

You can review monitor sets and SNMP set performance results, *with or without creating alarms*, using:

- Monitor > [Live Counter](#) (page 201)
- Monitor > [Monitor Log](#) (page 267)
- Monitor > [SNMP Log](#) (page 284)
- Monitor > Dashboard > [Network Status](#) (page 193)
- Monitor > Dashboard > [Group Alarm Status](#) (page 194)

- Monitor > Dashboard > [Monitoring Set Status](#) (page 194)
- Info Center > [Reports](#) (page 149) > Monitoring > Logs

**Note:** You must run [Update Lists by Scan](#) (page 203) for each machine ID you assign a monitor set, to ensure a complete list of monitoring definitions exists on the VSA to monitor that machine.

## Reviewing Performance Data using Quick Sets

A [Quick Status](#) feature enables you to select *any* monitor set counter, service or process from *any* machine ID and add it to the same single display window. Using [Quick Status](#), you can quickly compare the performance of the same counter, service or process on different machines, or display selected counters, services and processes from different monitor sets all within a single view. SNMP sets provide a similar [Quick Status](#) view for selected SNMP objects. *Any Quick Status view you create exists only for the current session.* The [Quick Status](#) window is accessed using Monitor > Dashboard > [Monitoring Set Status](#) (page 194), then clicking the [Quick Status](#) link or the [Quick Status](#) icon .

## Reviewing Performance Data using Machine Status or Device Status

A [Machine Status](#) feature enables you to select any monitor set counter, service or process *for a single machine ID* and add it to the same single display window. Unlike the Quick Status window, *a Machine Status view persists from one session to the next.* SNMP sets display a similar window called the [Device Status](#) window for selected SNMP objects. The Machine Status window and Device Status window are accessed using Monitor > Dashboard > [Monitoring Set Status](#) (page 194), then clicking the machine/device status icon .

## Suspending Alarms

The triggering of alarms can be suspended. The [Suspend Alarms](#) page suppresses [alarms](#) (page 585) for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms.*

## Group Alarms

Alert, system check, and log monitoring alarms are automatically assigned to a [group alarm](#) category. If an alarm is triggered, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the [Group Alarm Status](#) (page 194) dashlet of the Monitor > [Dashboard List](#) page. You can create new groups using the [Group Alarm Column Names](#) tab in Monitor > [Monitor Lists](#) (page 202). Group alarm column names are assigned to monitor sets using [Define Monitor Set](#) (page 206).

---

# Dashboard List

[Info Center](#) > [Dashboard List](#)

[Monitor](#) > [Dashboard List](#)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center
- Similar information is provided using [Monitor](#) > [Alarm Summary](#) (page 198) and [Info Center](#) > [Reports](#) > [Monitor Alarm Summary](#) (page 167).

The [Dashboard List](#) page is the VSA's primary method of visually displaying monitoring data, including triggered alarm conditions. The [Dashboard List](#) page maintains configurable monitoring windows called [Dashboard Views](#). Each dashboard contains one or more panes of monitoring data called [Dashlets](#). Each VSA user can create their own customized dashboards.

## Adding Dashboard Views and Dashlets

To add a new dashboard:

## Monitor

1. Click  to create a new **Dashboard View**. The new dashboard displays in a popup window.
2. Enter a **Title** and **Description** for your new dashboard.
3. Click the **Add Dashlets** tab. A side panel displays a list of dashlets. These choices include:
  - **Alarm List** (page 191)
  - **Alarm Network Status** (page 191)
  - **Alarm Rotator** (page 193)
  - **Alarm Ticker** (page 193)
  - **Network Status** (page 193)
  - **Group Alarm Status** (page 194)
  - **Monitoring Set Status** (page 194)
  - **Monitor Status** (page 196)
  - **Machines Online** (page 196)
  - **Top N - Monitor Alarm Chart** (page 197)
  - **KES Status** (page 197)
  - **KES Threats** (page 197)
4. Check as many checkboxes as you like, then click the **Add** button. The side panel closes and the **Dashlets** display in the **Dashboard View**.
5. Move and resize the **Dashlets** within the **Dashboard View**.
6. Click the **Delete** tab to delete dashlets already displayed in the **Dashboard View**.
7. Click  to save the **Dashboard View**. Click  to save the **Dashboard View** using a different title and description.
8. Click **Share** to share this **Dashboard View** with other users, user roles or to make it public for all users to use and edit.
9. Click **Take Ownership** to take ownership of a **Dashboard View**. This option only displays for **master role users** (page 600).

## Configuring Dashlet Options

You can size and position each dashlet within the **Dashboard View**. You can also access additional configuration options for each dashlet by clicking the configure icon  located in the upper left hand corner of the dashlet. Common configuration options include:

- **Show Title Bar** - If checked, displays the dashlet with a title bar.
- **Title** - Specifies the title of the dashlet.
- **Refresh Rate** - Specifies how often the data in the dashlet is refreshed.
- **Machine** - Filters the dashlet by machine ID. Include an asterisk (\*) wildcard with the text you enter to match multiple records.
- **Machine Group** - Filters the dashlets by group ID. Select <All Groups> to see all groups you are authorized to see.

**Note:** Dashlets are unaffected by the *main machine ID / machine group filter* (page 592) at the top of the VSA page.

## Add Dashboard

Click  to create a new dashboard. The new dashboard displays in a popup window.

## Title

Enter a title for your dashboard and click the filter icon  to filter the list of dashboards listed in the paging area. Include an asterisk (\*) wildcard with the text you enter to match multiple records. Enter a different title to rename the dashboard.

## My Dashboards

If checked, only the dashboards you are the owner of display.

## View

Displays the view icons available for each dashboard.

-  - Click to view this dashboard.
-  - Click to configure this dashboard.
-  - Click to delete this dashboard.

## Owner

The owner of the dashboard.

**Note:** You must take ownership of the dashboard to modify it.

## Title

The name of the dashboard.

## Description

The description of the dashboard.

## Load on Startup

If checked, this dashboard displays when the user logs in. Choices apply only to the currently logged in user.

## Alarm List

### Dashboard List > Alarm List

The **Alarm List** dashlet displays all alarms for all machine IDs matching the dashlet's machine ID/group ID filter. The display lists the most recent alarms first. By default, alarms generated within the **last 24 hours** are **highlighted in red**. Alarms generated within the **last week** are **highlighted in yellow**. The color coding lets you quickly distinguish alarms you may not have examined yet. The color coding is customizable using **Dashboard Settings** (*page 197*).

Each alarm contains a link to create or display a **Ticket** associated with the alarm.

## Alarm Network Status

### Dashboard List > Alarm Network Status

Initially the **Alarm Network Status** dashlet displays each machine group as an icon. You can click any group icon to display the machines within that group. If a machine has even a single **Open** alarm, then the icon for that machine displays a red exclamation point. Click any machine icon to display an **Alarm Summary Window** (*page 192*) of **Open** alarms for that machine.

## Alarm Summary Window

[Dashboard List](#) > [Alarm Network Status](#)

[Dashboard List](#) > [Group Alarm Status](#)

[Dashboard List](#) > [Monitor Set Status](#)

The **Alarm Summary** window displays a filtered list of alarm log records. The filtering depends on how you accessed the window. An alarm listed in the alarm log does not represent the *current state* of a machine or device, rather it is a *record* of an alarm that has occurred *in the past*. An alarm log record remains `Open` until you close it.

**Note:** Within a dashlet, the Alarm Summary window displays *only Open alarm log records*. If you attempt to filter alarms using the `Closed` status within a dashlet, the dashlet will reset your selection to `Open`. Closing an alarm makes it disappear from this dashlet's alarm summary list. You can review both `Open` and `Closed` alarms using the [Alarm Summary \(page 198\)](#) page.

### Filtering Alarms

Select or enter values in one or more of the following **Alarm Filter** fields. The filtering takes effect as soon as you select or enter a value.

- **Alarm ID** - A specific alarm ID.
- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Alarm State** - `Open` or `Closed`. You can only select the `Open` status for an alarm listed in a dashlet **Alarm Summary Window**.
- **Alarm Type** - Alarm or Trending.
- **Alarm Text** - Text contained in the alarm. Bracket text with asterisks, for example: `*memory*`
- **Filter Alarm Count** - The number of alarms displayed using the current filter criteria.

### Closing Alarms

You can close alarm log records in one of two ways:

- Click the `Open` link in the **State** column of the **Alarm Summary** window.

Or:

1. Set the **Alarm State** drop-down list to `Closed`.
2. Select one or more alarms listed in the paging area.
3. Click the **Update** button.

### Deleting Alarms

1. Select one or more alarms listed in the paging area.
2. Click the **Delete...** button.

### Adding Notes

1. Enter a note in the **Notes** field.
2. Select one or more alarms listed in the paging area.
3. Click the **Update** button.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Alarm ID

Lists a system-generated and unique ID for each alarm. The expand icon  can be clicked to display specific alarm information.

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404). Each dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

## Alarm Date

The date and time the alarm was created.

## Type

The type of monitor object: Counter, Process, Service, SNMP, Alert, System Check, Security and Log Monitoring.

## Ticket

If a ticket has been generated for an alarm a [Ticket ID](#) link displays. Clicking this link displays the ticket in the Ticketing > [View Ticket](#) (page 438) page. If no ticket has been generated for an alarm a [New Ticket...](#) link displays. Click this link to create a ticket for this alarm.

## Name

The name of the monitoring object.

## Alarm Rotator

[Dashboard List](#) > [Alarm Rotator](#)

The [Alarm Rotator](#) dashlet displays current alarms that have occurred within the last 10 minutes. Each alarm displays one at a time, in a rotating fashion, for 10 seconds. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

## Alarm Ticker

[Dashboard List](#) > [Alarm Ticker](#)

The [Alarm Ticker](#) dashlet displays current alarms that have occurred within a specified period. Each alarm displays one at a time, in a "ticker-tape" fashion, for 10 seconds. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

## Network Status

[Dashboard List](#) > [Network Status](#)

The [Network Status](#) dashlet is specific for machines assigned *monitor sets* or devices assigned *SNMP sets*. This dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

The value of this dashlet is that you can see the *current state* of monitor sets on machines or SNMP

## Monitor

sets on devices *dynamically*.

Initially the **Network Status** dashlet displays each machine group as an icon. You can click any group icon to display the machines and SNMP devices within that group. If even a single monitor set or SNMP set is in an alarm state, then the icon for that machine or device displays a red exclamation point. Click any machine icon or device icon to display a list of monitor set alarms or SNMP set alarms that are *currently* outside their alarm thresholds. Alarms in this list are automatically removed as soon as the monitor set or SNMP set returns to a "no alarm" state.

## Dismissed

You can manually force an alarm to return to a "no alarm" state by clicking the **Dismiss** link for that alarm. The "alarm" state will reappear again if the monitor set or SNMP set crosses its alarm threshold again. The timing of the reappearance depends on the alarm interval criteria defined for that monitor set or SNMP set.

**Note:** Dismissing an alarm *state* should not be confused with the **Open** or **Closed** status of an alarm *record* entered in the alarm log, which is displayed, for example, using the **Alarm Summary Window** (page 192). Alarm log entries can remain **Open** indefinitely, long after the alarm state has returned to "no alarm".

## Group Alarm Status

Dashboard List > Group Alarm Status

The **Group Alarm Status** dashlet summarizes the alarm status of all **group alarm** (page 590) categories, for all machine IDs matching the *dashlet's* unique machine ID/group ID filter. Alert, system check, and log monitoring alarms are automatically assigned to a **group alarm** category. If an alarm is triggered, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the **Group Alarm Status** (page 194) dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > **Monitor Lists** (page 202). Group alarm column names are assigned to monitor sets using **Define Monitor Set** (page 206).

**Note:** Do not confuse *group alarm categories* with *machine group IDs*.

- Click the **machine group ID** link to display the group alarm status of all machine IDs and SNMP device IDs included in that machine group ID.
- Click the **Machine ID/SNMP Device ID** link to display a **Monitor Set Status** (page 194) window for the machine ID and any SNMP devices linked to it.
- Click any red icon  in the table to display the **Alarm Summary Window** (page 192) for that combination of *group alarm category and machine group ID* or *group alarm category and machine ID*.
- Click **Filter...** to filter a dashlet by group alarm category or by machine group ID. Click **Reset** to return a filtered dashlet back to its default. You can also re-order the display of group alarm categories.

## Monitoring Set Status

Dashboard List > Monitoring Set Status

- You can also display a **Monitoring Set Status** dashlet using a **Group Alarm Status** dashlet, by clicking a machine group ID link, then a machine ID link.

The **Monitoring Set Status** dashlet displays all alarms assigned to a machine ID, whether created by **monitor set** (page 593), **alert** (page 585), **system check** (page 599), **SNMP set** (page 212), or **Log Monitoring** (page 591). Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

## Display only alarmed monitor objects

If checked, only alarmed monitor objects are displayed in the list.

## Display only alarmed machines

If checked, only alarmed machines are displayed in the list.

## First Row of Information

The first row of information displays:

- The **check-in status** (on page 588) icon - Click to display the **Live Connect** (page 380) window. Alt-click to display the **Machine Summary** (page 137) page.
- The machine status icon  - Click to display the **Machine Status** (page 196) popup window. This window enables you to set up a permanent display of charts or tables of monitor set objects for a specific machine ID. Applies to monitor set objects only—not alerts, system-checks or SNMP sets.
- The expand icon  - Click to display all alarms assigned to a machine ID.
- The collapse icon  - Click to display only the header description of each alarm assigned to a machine ID.
- The **machine ID.group ID** (page 592).

## Monitor Sets

If a monitoring set is assigned to a machine ID, the following displays below the name of the monitor set:

- The triggered alarm  or no-alarm  status of the monitoring set.
- The expand icon  - Click to display collection and threshold information.
- The **Quick Status** link or the quick chart icon  - Click to display a **Quick Status Monitor** popup window. This window provides a quick chart of the monitor set object you click. Clicking a *different* quick chart icon within the same monitor set adds that monitor set object to the **Quick Status Monitor** window. Quick chart selections are not permanently saved between sessions. Use the **Machine Status** (page 196) icon  to permanently save chart display selections.
- The monitoring log icon  - Click to display the **monitoring log** (page 267) for this single alarm counter in a popup window.
- The live monitoring log icon  - Click to display current, ongoing counter log information in a popup window.
- The monitor set object name.
- For triggered alarms, the **Alarm** hyperlink displays. Click to display the **Alarm Summary Window** (page 192). The **Alarm Summary Window** is restricted to just `Open` alarms for the selected monitor set object and machine ID.

## Alerts

If an alert is assigned to a machine ID, the following displays with each alert:

- The triggered alarm  or no-alarm  status of the alert.
- The alert type.
- For triggered alarms, the **Alarm** hyperlink displays. Click to display the **Alarm Summary Window** (page 192). The **Alarm Summary Window** is restricted to just `Open` alerts for the selected machine ID.

## System Checks

If a system check is assigned to a machine ID, the following displays with each system check:

- The triggered alarm  or no-alarm  status of the system check.
- The system check type.

## Monitor

- For triggered alarms, the **Alarm** hyperlink displays. Click to display the **Alarm Summary Window** (page 192). The **Alarm Summary Window** is restricted to just `Open` system checks for the selected machine ID.

## SNMP Devices

If a SNMP set is assigned to a SNMP device, the following displays with each SNMP set object:

- The device status icon  - Click to set up a permanent display of charts or tables of monitor set objects for a specific SNMP device. Displays the **Device Status** (page 196) popup window.
- The IP address of the SNMP device.
- The name of the SNMP device.
- The name of the SNMP set assigned to the SNMP device. The following displays with each SNMP set:
  - The triggered  or no-alarm  status of the SNMP set.
  - The expand icon  - Click to display collection and threshold information.
  - The monitoring log icon  - Click to display the **SNMP log** (page 284) for this single alarm counter in a popup window.
  - The SNMP set object name.
  - For triggered alarms, the **Alarm** hyperlink displays. Click to display the **Alarm Summary Window** (page 192). The **Alarm Summary Window** is restricted to just `Open` alarms for the selected SNMP set object and SNMP device.

## Machine Status

Dashboard List > Monitor Set Status > Machine Status icon 

The **Machine Status** popup window selects and displays charts or tables for **monitor set** (page 593) objects. The setup is specific for each machine ID and can be saved permanently. Applies to monitor set objects only. Monitor sets must be assigned to a machine ID before using this window.

- Click the **Setup...** button to select monitoring objects to display and to set the chart or table format.
- Click the **Save Position** button to save the selection and format of monitoring objects on the **Monitor Set Status** popup window.

## Device Status

Dashboard List > Monitor Set Status > Machine Status icon 

The **Device Status** popup window selects and displays charts or tables for **SNMP devices** (page 597). The setup is specific for each SNMP device and can be saved permanently.

- Click the **Setup...** button to select monitoring objects to display and to set the chart or table format.
- Click the **Save Position** button to save the selection and format of monitoring objects on the **Monitor Set Status** popup window.

## Monitor Status

Dashboard List > Monitor Status

The **Monitor Status** dashlet displays a bar chart showing the number of alarms created for the selected time interval. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. This dashlet can be customized using Monitor > **Dashboard Settings** (page 197).

## Machines Online

Dashboard List > Machines Online

The **Machines Online** chart shows the percentage of servers and workstations online. Applies to all

machine IDs matching the *dashlet's* unique machine ID/group ID filter. This dashlet can be customized using Monitor > [Dashboard Settings](#) (page 197).

## Top N - Monitor Alarm Chart

[Dashboard List](#) > [Top N - Monitor Alarm Chart](#)

The [Top N - Monitor Alarm Chart](#) dashlet displays a bar chart showing which machines have the *most* alarms for the selected time interval. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The chart shows up to 10 machines. This dashlet can be customized using Monitor > [Dashboard Settings](#) (page 197).

## KES Status

[Dashboard List](#) > [KES Status](#)

The [KES Status](#) dashlet displays different views of the security status of machine IDs using Endpoint Security protection. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The three views of security status are:

- [Machine Configuration](#)
- [Scan Details](#)
- [Profile Chart](#)

**Note:** This dashlet does not display unless the Endpoint Security add-on module is installed for the VSA.

## KES Threats

[Dashboard List](#) > [KES Threats](#)

The [KES Threats](#) dashlet displays different views of the security threats reported for machine IDs using Endpoint Security protection. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The three views of security threats are:

- [Most Recent](#)
- [Most Common](#)
- [Profile Chart](#)

**Note:** This dashlet does not display unless the Endpoint Security add-on module is installed for the VSA.

---

## Dashboard Settings

[Info Center](#) > [Settings](#)

[Monitor](#) > [Dashboard Settings](#)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Settings](#) page enables you to customize controls for dashlets.

- [Turn notification sounds on or off for all popup monitoring windows](#) - Applies only to the [Monitor Set Status](#) (page 194) dashlet.
- The [Chart Total Monitor Alarms](#) and [Chart Top N Monitor Alarms](#) title and background colors are customizable. Each chart parameter is customizable, this includes the chart time interval and the number of machines referenced by the [Chart Top N Monitor Alarms](#).
- The [Customize machines online chart zone](#) specifies two percentages to create three zones of machines online:

## Monitor

- The percentage of machines online, below which represents an alarm condition.
- The additional percentage of machines online, below which represents a warning condition.
- **Show refresh time**
- **Custom Dashboard Skin** - Select the border and titlebar style you want dashlets to display.

---

# Alarm Summary

## Monitor > Alarm Summary

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*
- Similar information is provided using *Monitor > Dashboard Lists (page 189)* and *Info Center > Reports > Monitor*.

The **Alarm Summary** page displays **alarms** (page 585) for all machine IDs that match the current **machine ID / group ID filter** (page 26). You can include additional filtering for listed alarms using fields in the **Alarm Filters** panel. You can also close alarms or re-open them and add notes to alarms.

## Filtering Alarms

Select or enter values in one or more of the following **Alarm Filter** fields. The filtering takes effect as soon as you select or enter a value.

- **Alarm ID** - A specific alarm ID.
- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Alarm State** - Open or Closed. You can only select the Open status for an alarm listed in a dashlet **Alarm Summary Window**.
- **Alarm Type** - Alarm or Trending.
- **Alarm Text** - Text contained in the alarm. Bracket text with asterisks, for example: *\*memory\**
- **Filter Alarm Count** - The number of alarms displayed using the current filter criteria.

## Closing Alarms

You can close alarm log records in one of two ways:

- Click the **Open** link in the **State** column of the **Alarm Summary** window.

Or:

1. Set the **Alarm State** drop-down list to **Closed**.
2. Select one or more alarms listed in the paging area.
3. Click the **Update** button.

## Deleting Alarms

1. Select one or more alarms listed in the paging area.
2. Click the **Delete...** button.

## Adding Notes

1. Enter a note in the **Notes** field.
2. Select one or more alarms listed in the paging area.
3. Click the **Update** button.

## Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Alarm ID

Lists a system-generated and unique ID for each alarm. The expand icon  can be clicked to display specific alarm information.

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404). Each dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

## Alarm Date

The date and time the alarm was created.

## Type

The type of monitor object: Counter, Process, Service, SNMP, Alert, System Check, Security and Log Monitoring.

## Ticket

If a ticket has been generated for an alarm a [Ticket ID](#) link displays. Clicking this link displays the ticket in the Ticketing > [View Ticket](#) (page 438) page. If no ticket has been generated for an alarm a [New Ticket...](#) link displays. Click this link to create a ticket for this alarm.

## Name

The name of the monitoring object.

---

# Suspend Alarms

## Monitor > Suspend Alarms

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Suspend Alarms](#) page suppresses [alarms](#) (page 585) for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms*. The list of machine IDs you can select depends on the [machine ID / group ID filter](#) (page 26).

## Clear All

Clears all time periods scheduled for suspending alarms for all selected machine IDs.

## Add / Replace

Click [Add](#) to add a schedule time period when alarms will be suspended for selected machine IDs. Click [Replace](#) to remove suspend alarm time periods currently assigned to selected machine IDs and assign them a new single time period to suspend alarms.

## Monitor

### Schedule

Click [Schedule](#) to schedule this task on selected machine IDs using the schedule options previously selected.

### Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

### Cancel

Clears a time period matching the date/time parameters for suspending alarms on selected machine IDs.

### Run recurring

Check the box to make this task a recurring task. Enter the number of periods to wait before running this task again.

### Suspend alarms

Select the duration of time during which alarms will be suspended.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Next Suspend

Lists the start times when machine ID alarms are scheduled to be suspended.

### Duration

Lists the duration of the time periods alarms are scheduled to be suspended.

### Recur

If recurring, displays the interval to wait before running the task again.

---

# Live Counter

## Monitor > Live Counter

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Live Counter** page displays live **performance counter** (page 596) data for a selected machine ID. Only machines IDs assigned one or more monitor sets using **Assign Monitoring** (page 261) are listed on this page. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 26).

Each specific **Live Counter** displays in a new window. Each window displays a bar chart with 75 data points containing the value of the counter object for the **Refresh Rate** specified. The chart refresh rate can be set between 3 and 60 seconds. The new data displays on the far right of the chart and the data moves from right to left as it ages.

Each bar within the chart displays in a specific color, which is determined by the alarm and warning thresholds of the monitor set counter object.

- **Red** - if alarming
- **Yellow** - if within warning threshold
- **Green** - if not alarming or not in warning threshold

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## (Machine.Group ID)

Lists the **Machine.Group IDs** (page 592) currently matching the **Machine ID / Group ID filter** (page 26) and that has been assigned one or more monitor sets. Click a machine ID to select a monitor set, refresh rate and one or more counters.

## Select Monitor Set

Select a monitor set.

## Refresh Rate

Enter a value from 3 to 60. This is the interval **Live Counter** uses to gather data.

## Select Counter

Lists the counters included in a selected monitor set. Click a counter link to display a **Live Counter** window for that counter.

---

# Monitor Lists

## Monitor > Monitor Lists

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Monitor Lists** page maintains the complete list of all objects, services and processes loaded on the KServer that are used to create **Monitor Sets** (page 204) and **SNMP Sets** (page 212). The **Monitor List** page also maintains user-defined **group alarms** (page 590).

**Note:** The **Counter Objects**, **Counters**, **Instances** and **Services** lists can be initially populated by using the **Update Lists by Scan** (page 203) page. Additionally these lists, as well as **Services** and **Processes**, can be populated with the import of a **Monitor Set** (page 204). **MIB OIDs** can be populated by using the **Add SNMP Object** (page 217) page or by the import of a **SNMP Set** (page 212).

## Counter Objects

This tab lists **counter objects** you can include in a **Monitor Set** (page 204). Monitor Set uses the **PerfMon** combination of **object/counter/instance** (page 596) to collect counter information.

**Note:** Counter Objects are the primary reference. The user needs to add a record of the counter object first, before adding records of the corresponding counters or instances.

## Counters

This tab lists **counters** you can include in a **Monitor Set** (page 204). Monitor Set uses the **PerfMon** combination of object/counter/instance to collect counter information.

## Counter Instances

This tab lists **counter instances** you can include in a **Monitor Set** (page 204). Monitor Set uses the **PerfMon** combination of object/counter/instance to collect counter information.

**Note:** Windows **PerfMon** requires that a counter object have at least one counter, but does not require an instance be available.

## Services

This tab lists Windows **services** you can include in a **Monitor Set** (page 204) to monitor the activity of Windows Services. This list can also be populated with the execution of the **Update Lists By Scan** (page 203) page or the import of a **Monitor Set** (page 204).

## Processes

This tab lists Windows **processes** you can include in a **Monitor Set** (page 204) to monitor the transition of a process to or from a running state. A process is equivalent to an application. The processes list is *not* populated via the **Update Lists by Scan** (page 203) feature. This list can be populated by the import of a **Monitor Set** (page 204).

## CMIB OIDs

This tab lists SNMP **MIB objects** you can include in **SNMP Sets** (page 212). SNMP sets monitor the activity of SNMP devices. This list can be populated with the import of a **SNMP Set** (page 212) or the execution of the **Add SNMP Object** (page 217) page. MIB objects are references to values that can be monitored on SNMP devices. Example: the MIB object `sysUptime` returns how much time has passed since the device was powered-up.

## SNMP Devices

This tab defines broad categories of SNMP devices called [Set SNMP Types](#) (page 287). This enables the convenient assignment of SNMP sets to multiple SNMP devices, based on their SNMP type. Assignment can be either automatic or manual. See [SNMP Services](#) below for more information.

## SNMP Services

This tab associates a `sysServicesNumber` with a SNMP type. A SNMP type is associated with a SNMP set using the [Automatic Deployment to](#) drop-down list in Monitor > SNMP Sets > [Define SNMP Set](#) (page 213). During a [LAN Watch](#) (page 272) SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a `sysServicesNumber` associated with a SNMP type used by those SNMP sets. This table comes with pre-defined SNMP types and `sysServicesNumbers` for basic devices. System updates and updates provided by customers themselves can update this table.

## Group Alarm Column Names

This tab maintains *user defined* [Group Alarm Column Names](#). Pre-defined [group alarm](#) (page 590) column names do not display here. Use [Monitor Sets](#) (page 204) and [Define Monitor Sets](#) (page 206) to assign a monitor set to any group alarm column name. Group alarms are displayed using the [Dashboard List](#) (page 189) page.

## Page Select

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Edit Icon

Click the edit icon  to edit the text of a list item.

## Delete Icon

Click the delete icon  to delete a list item.

---

# Update Lists By Scan

## Monitor > Update Lists By Scan

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Update Lists by Scan](#) page scans one or more machine IDs and returns lists of counter objects, counters, instances and services to select from when creating or editing a monitor set. Lists display in the Monitor > [Monitor Lists](#) (page 202) page. Typically only a handful of machines of each operating system type need to be scanned to provide a set of comprehensive lists.

[Update Lists by Scan](#) also updates the list of event types available for monitoring using Monitoring > Alerts > [Event Logs](#) (page 234). You can see the list of event types available by displaying the Agent > [Event Log Settings](#) (page 37) page.

## Schedule

Click [Schedule](#) to display the [Scheduler](#) window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

## Monitor

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

## Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

## Next Scan

This timestamp shows the next scheduled scan. Overdue date/time stamps display as **red text with yellow highlight**. A green  checkmark indicates the scan is recurring.

---

# Monitor Sets

## Monitor > Monitor Sets

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Monitor Sets** page adds, imports or modifies monitor sets. Sample monitor sets are provided.

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 596), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the

monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Update monitor set counter objects, instances and counters by source machine ID using Monitor > **Update Lists by Scan** (page 203).

**Note:** You must run **Update Lists by Scan** (page 203) for each machine ID you assign a monitor set, to ensure a complete list of monitoring definitions exists on the VSA to monitor that machine.

2. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 202).
3. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 204).
4. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 261).
5. Optionally customize standard monitor sets as *individualized monitor sets*.
6. Optionally customize standard monitor sets using *Auto Learn*.
7. Review monitor set results using:
  - Monitor > **Monitor Log** (page 267)
  - Monitor > **Live Counter** (page 201)
  - Monitor > Dashboard > **Network Status** (page 193)
  - Monitor > Dashboard > **Group Alarm Status** (page 194)
  - Monitor > Dashboard > **Monitoring Set Status** (page 194)
  - Info Center > Reports > Monitor > Monitor Set Report
  - Info Center > Reports > Monitor > Monitor Action Log

## Sample Monitor Sets

The VSA provides a growing list of sample monitor sets. The names of sample monitor sets begin with ZC. You can modify sample monitor sets, but its better practice to copy a sample monitor set and customize the copy. Sample monitor sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.

## Monitoring using Macintosh OSX

Macintosh OSX supports process monitoring only. See System Requirements.

## Folder Trees

Monitor sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

### Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

### When a Folder is Selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

## Monitor

**Note:** See guidelines for share rights to objects within folder trees in the [Folder Rights \(page 119\)](#) topic.

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New Monitor Set** - Opens the **Define Monitor Set (page 206)** window to create a new monitor set in the selected folder of the folder tree.
- **Import Monitor Set** - Imports a monitor set.
- **Take Ownership - Takes ownership (page 119)** of a folder you do not own. This option only displays for **master role users (page 600)**.

### When a Monitor Set is Selected

- **Copy Monitor Set** - Copies the selected monitor set.
- **Export Monitor Set** - Exports the selected procedure.
- **Delete Monitor Set** - Deletes the selected procedure.

## Creating Monitor Sets

1. Select a folder in the middle pane.
2. Click the **New Monitor Set** button.
3. Enter a name.
4. Enter a description.
5. Select a **group alarm (page 590)** category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the **Monitor Lists (page 202)** page. Group alarms display on the **Dashboard List (page 189)** page.
6. Click **Save**. The **Define Monitor Sets (page 206)** window displays.

**Note:** Sample monitor sets do not display in the **Assign Monitoring (page 261) > Select Monitor Set** drop-down list. Create a copy of a sample monitor set by selecting the sample set in **Monitor Sets (page 204)** and clicking the **Save As** button. Your copy of the sample monitor set will display in the drop-down list. In the SaaS version of the VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

## Define Monitor Sets

### Monitor > Monitor Sets

- Select a monitor set in a folder.

The **Define Monitor Sets** window maintains a set of counter objects, counters, counter instances, services and processes included in a monitor set. This collection is drawn from a "master list" maintained using **Monitor Lists (page 202)**. Sample monitor sets are provided.

## Monitor Sets

A monitor set is a set of **counter objects, counters, counter instances, services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter (page 596)**, service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Update monitor set counter objects, instances and counters by source machine ID using Monitor > [Update Lists by Scan](#) (page 203).

**Note:** You must run [Update Lists by Scan](#) (page 203) for each machine ID you assign a monitor set, to ensure a complete list of monitoring definitions exists on the VSA to monitor that machine.

2. Optionally update monitor set counter objects, instances and counters manually and review them using [Monitor Lists](#) (page 202).
3. Create and maintain monitor sets using Monitor > [Monitor Sets](#) (page 204).
4. Assign monitor sets to machine IDs using Monitor > [Assign Monitoring](#) (page 261).
5. Optionally customize standard monitor sets as *individualized monitor sets*.
6. Optionally customize standard monitor sets using *Auto Learn*.
7. Review monitor set results using:
  - Monitor > [Monitor Log](#) (page 267)
  - Monitor > [Live Counter](#) (page 201)
  - Monitor > Dashboard > [Network Status](#) (page 193)
  - Monitor > Dashboard > [Group Alarm Status](#) (page 194)
  - Monitor > Dashboard > [Monitoring Set Status](#) (page 194)
  - Info Center > Reports > Monitor > Monitor Set Report
  - Info Center > Reports > Monitor > Monitor Action Log

Click the following tabs to define monitor set details.

- [Counter Thresholds](#) (page 208)
- [Services Check](#) (page 210)
- [Process Status](#) (page 210)
- [Monitor Icons](#) (page 211)

### Monitor Set Name

Enter a descriptive name for the monitor set that helps you identify it in monitor set lists.

### Monitor Set Description

Describe the monitor set in more detail. The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

### Group Alarm Column Name

Assign this monitor set to a [Group Alarm Column Name](#). If a monitor set alarm is triggered, the [group alarm](#) (page 590) it belongs to is triggered as well. Group alarms display in the [Group Alarm Status](#) (page 194) pane of the Monitor > [Dashboard List](#) page.

### Save

Saves changes to a record.

### Save As

Saves a record using a new name.

### Export Monitor Set...

Click the [Export Monitor Set...](#) link to display the procedure in XML format in the [Export Monitor Sets](#) popup window. You can copy it to the clipboard or download it to a text file.

## Counter Thresholds

### Monitor > Monitor Sets

- Select a monitor set in a folder, then Counter Thresholds

The **Counter Thresholds** tab defines alarm conditions for all performance objects/instances/counters associated with a monitor set. These are the same performance objects, instances and counters displayed when you run `PerfMon.exe` on a Windows machine.

### Performance Objects, Instances and Counters

When setting up counter thresholds in **monitor sets** (page 593), it's helpful to keep in mind exactly how both Windows and the VSA identify the components you can monitor:

- **Performance Object** - A logical collection of counters that is associated with a resource or service that can be monitored. For example: processors, memory, physical disks, servers each have their own sets of predefined counters.
- **Performance Object Instance** - A term used to distinguish between multiple performance objects of the same type on a computer. For example: multiple processors or multiple physical disks. The VSA lets you skip this field if there is only one instance of an object.
- **Performance Counter** - A data item that is associated with a performance object, and if necessary, the instance. Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

### Edit icon

Click the edit icon  next to row to edit the row.

### Delete Icon

Click the delete icon  to delete this record.

### Add / Edit

Click **Add** or the edit icon  to use a wizard that leads you through the six steps required to add or edit a performance counter.

1. Select a **Object**, **Counter** and, if necessary, an **Instance** using their respective drop-down lists.
  - If only one instance of a performance object exists, the **Instance** field can usually be skipped.
  - The drop-down lists used to select performance objects, counters, and instances are based on the "master list" maintained using the **Monitor Lists** (page 202) page. If an object/instance/counter does not display in its respective drop-down list, you can add it manually using **Add Object**, **Add Counter**, and **Add Instance**. You can also update the "master list" of all objects, instances and counters by scanning specific machine IDs using **Update Lists By Scan** (page 203). Once the update is completed, the drop lists should be populated with the options you require.
  - When multiple instances exist, you often have the option of using an instance called `_Total`. The `_Total` instance means you want to monitor the *combined* value of all the other instances of a performance object *as a single counter*. The `_Total` can be used as a kind of "wildcard instance". Without the `_Total` instance you would have to specify each instance by its exact name, which makes applying the same monitor set to multiple machines difficult. The true benefit of the `_Total` instance is determining if there *are any performance issues for any instance of this object at all*. Once you know that you can investigate the specific cause.

- When multiple instances exist, you sometimes have the option of using an instance called \*ALL. The \*ALL instance means you want to monitor all instances for the same performance object *using individual counters*.
2. Optionally change the default counter object **Name** and **Description**.
  3. Select the log data collected. If the returned value is numeric, you can minimize unwanted log data by setting a collection operator just over or just under the collection threshold.
    - **Collection Operator** - For character string return values, the options are Changed, Equal or NotEqual. For numeric return values, the options are Equal, NotEqual, Over, or Under.
    - **Collection Threshold** - Set a fixed value that the returned value is compared to, using the selected **Collection Operator**, to determine what log data is collected.
    - **Sample Interval** - Defines how frequently the data is sent by the agent to the KServer.
  4. Specify when an alarm condition is encountered.
    - **Alarm Operator** - For character string return values, the options are Changed, Equal or NotEqual. For numeric return values, the options are Equal, NotEqual, Over or Under.
    - **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alarm condition is encountered.
    - **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alarm condition. Many alarm conditions are only alarming if the level is sustained over a long period of time.
    - **Ignore additional alarms for** - Suppress additional alarm conditions for this same issue for this time period. This reduces the confusion of many alarm conditions for the same issue.
  5. **Warn when within X% of alarm threshold** - Optionally display a warning alarm condition when the returned value is within a specified percentage of the **Alarm Threshold**. The default warning icon is a yellow traffic light icon 🟡. See **Monitor Icons** (page 211).
  6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alarm condition will occur.
    - **Trending Activated?** - If yes, a linear regression trendline is calculated based on the last 2500 data points logged.
    - **Trending Window** - The time period used to extend the calculated trendline into the future. If the predicted trendline exceeds the alarm threshold within the future time period specified, a trending alarm condition is generated. Typically a trending window should be set to the amount of time you need to prepare for an alarm condition, if it occurs. Example: a user may want 10 days notice before a hard drive reaches the alarm condition, to accommodate ordering, shipping and installing a larger hard drive.
    - **Ignore additional trending alarms for** - Suppress additional trending alarm conditions for this same issue for this time period.
    - By default, trending alarms display as an orange icon 🟠. You can change this icon using the **Monitor Icons** (page 211) tab.

Warning status alarm conditions and trending status alarm conditions don't create alarm entries in the alarm log, but they change the image of the alarm icon in various display windows. You can generate a trending alarm report using Reports > Monitor.

## Next

Moves to the next wizard page.

## Previous

Moves back to the previous wizard page.

## Monitor

### Save

Saves changes to a record.

### Cancel

Ignores changes and returns to the list of records.

## Services Check

### Monitor > Monitor Sets

- Select a monitor set in a folder, then **Services Check**

The **Services Check** tab defines alarms conditions for a service if the service on a machine ID has stopped, and optionally attempts to restart the stopped service. *The service must be set to automatic to be restarted by a monitor set.*

### Select Pages

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

### Edit icon

Click the edit icon  next to row to edit the row.

### Delete Icon

Click the delete icon  to delete this record.

### Add / Edit

Click **Add** or the edit icon  to maintain a **Services Check** record.

1. **Service** - Selects the service to be monitored from the drop-down list.
  - The drop-down list is based on the "master list" maintained using the **Monitor Lists** (page 202) page. If a service does not display in the drop-down list, you can add it manually using **Add Service**. You can also update the "master list" by scanning specific machine IDs using **Update Lists By Scan** (page 203).
  - Select the \*ALL selection to monitor all services on a monitored machine.
2. **Description** - Describes the service and the reason for monitoring.
3. **Restart Attempts** - The number of times the system should attempt to restart the service.
4. **Restart Interval** - The time period to wait between restart attempts. Certain services need more time.
5. **Ignore additional alarms for** - Suppresses additional alarm conditions for the specified time period.

### Save

Saves changes to a record.

### Cancel

Ignores changes and returns to the list of records.

## Process Status

### Monitor > Monitor Sets

- Select a monitor set in a folder, then **Process Status**

The **Process Status** tab defines alarm conditions based on whether a process has started or stopped on a machine ID.

### Select Pages

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

### Edit icon

Click the edit icon  next to row to edit the row.

### Delete Icon

Click the delete icon  to delete this record.

### Add / Edit

Click **Add** or the edit icon  to maintain a **Process Status** record.

1. **Process** - Selects the process to be monitored from the drop-down list. The drop-down list is based on the "master list" maintained using the **Monitor Lists** (page 202) page. If a process does not display in the drop-down list, you can add it manually using **Add Process**. You can also update the "master list" by scanning specific machine IDs using **Update Lists By Scan** (page 203).
2. **Description** - Describes the process and the reason for monitoring.
3. **Alarm on Transition** - Triggers an alarm condition when a process (application) is started or stopped.
4. **Ignore additional alarms for** - Suppresses additional alarm conditions for the specified time period.

### Save

Saves changes to a record.

### Cancel

Ignores changes and returns to the list of records.

## Monitor Icons

### Monitor > Monitor Sets

- Select a monitor set in a folder, then **Monitor Icons**

The **Monitor Icons** tab selects the monitor icons that display in the **Monitor Log** (page 267) page when various alarm states occur.

- **Select Image for OK Status** - The default icon is a green traffic light .
- **Select the Image for Alarm Status** - The default icon is a red traffic light .
- **Select Image for Warning Status** - The default icon is a yellow traffic light .
- **Select the Image for Trending Status** - The default icon is an orange traffic light .
- **Select the Image for Not Deployed Status** - The default icon is a grey traffic light .

### Save

Saves changes to a record.

### Upload additional monitoring icons

Select the **Upload additional monitoring icons** link to upload your own icons to the status icon drop-down lists.

## Monitor

## Restore

Sets all monitor icons back to their defaults.

---

# SNMP Sets

## Monitor > SNMP Sets

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

**SNMP Sets** adds, imports or modifies a SNMP set. A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 597). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 597) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 598) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 272).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 276). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 284) or **Dashboard List** (page 189).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 202).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 212).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 217).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 287).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 286).

**Note:** Certain command line functions from the Net-SNMP suite of applications are used to implement SNMP v1 and SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.

## Monitoring using Macintosh OSX

Macintosh OSX supports SNMP monitoring. See System Requirements.

## Folder Trees

SNMP sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

*Always Available*

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

#### When a Folder is Selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

**Note:** See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 119) topic.

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New SNMP Set** - Opens the **Define SNMP Set** (page 213) window to create a new monitor set in the selected folder of the folder tree.
- **Import SNMP Set** - Imports a monitor set.
- **Take Ownership - Takes ownership** (page 119) of a folder you do not own. This option only displays for **master role users** (page 600).

#### When a Monitor Set is Selected

- **Delete Monitor Set** - Deletes the selected procedure.

### Creating SNMP Sets

1. Select a folder in the middle pane.
2. Click the **New SNMP Set** button.
3. Enter a name.
4. Enter a description.
5. Select an **SNMP type** (page 287) from the **Automatic deployment to** drop-down list. If a LAN Watch detects this type of SNMP device the system automatically begins monitoring the SNMP device using this SNMP set.
6. Select a **group alarm** (page 590) category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the **Monitor Lists** (page 202) page. Group alarms display on the **Dashboard List** (page 189) page.
7. Click **Save**. The **Define SNMP Set** (page 213) window displays.

**Note:** Sample SNMP sets do not display in the **Assign SNMP** (page 276) > **Select SNMP Set** drop-down list. Create a copy of a sample SNMP set by selecting the sample set in **SNMP Sets** (page 212) and clicking the **Save As** button. Your copy of the sample SNMP set will display in the drop-down list. In the SaaS version of the VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

## Define SNMP Set

### Monitor > SNMP Sets

- Select a SNMP set in a folder.

The **Define SNMP Set** page maintains a collection of MIB objects included in a SNMP set.

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 597). The SNMP protocol is used because an agent cannot be installed on the device. You can

## Monitor

assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 597) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 598) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 272).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 276). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 284) or **Dashboard List** (page 189).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 202).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 212).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 217).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 287).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 286).

**Note:** Certain command line functions from the Net-SNMP suite of applications are used to implement SNMP v1 and SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.

Click the following tabs to define SNMP set details.

- **SNMP Sets** (page 215)
- **SNMP Icons** (page 218)

### SNMP Monitor Set Name

Enter a descriptive name for the SNMP set that helps you identify it in SNMP set lists.

### SNMP Monitor Set Description

Describe the SNMP set in more detail. The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

### Automatic Deployment to

Selecting a type automatically assigns a newly discovered SNMP device to a **Set SNMP Type** (page 287) when performing a **LAN Watch** (page 272) function.

### Group Alarm Column Name

Assign this SNMP set to a **Group Alarm Column Name**. If a SNMP set alarm is triggered, the group alarm it belongs to is triggered as well. Group alarms display in the Group Alarm Status pane of the **Dashboard List** (page 189) page.

## Save

Saves changes to a record.

## Save As

Saves a record using a new name.

## Export SNMP Set...

Click the [Export SNMP Set...](#) link to display the procedure in XML format in the [Export Monitor Sets](#) popup window. You can copy it to the clipboard or download it to a text file. SNMP sets can be *imported* using the [SNMP Sets](#) (page 212) page.

## SNMP Set Details

Monitor > Define SNMP Set

- Select a SNMP set in a folder, then [SNMP Sets](#)

The [SNMP Sets](#) tab enables you to maintain all MIB objects associated with a SNMP set.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

### Edit icon

Click the edit icon  next to row to edit the row.

### Delete Icon

Click the delete icon  to delete this record.

### Add / Edit

Click [Add](#) or the edit icon  to use a wizard that leads you through the six steps required to add or edit the monitoring of a MIB object.

1. Add the object/version/instance combination required to retrieve information from a SNMP device.
  - **MIB Object** - Select the [MIB object](#) (page 597). Click [Add Object](#) (page 217) to add a MIB object that currently does not exist on the [Monitor Lists](#) (page 202) page.
  - **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
  - **SNMP Instance** - The last number of an object ID may be expressed as a table of values instead of as a single value. If the instance is a single value, enter 0. If the instance is a table of values, enter a range of numbers, such as 1-5, 6 or 1, 3, 7.

**Note:** If you're not sure what numbers are valid for a particular SNMP instance, select a machine ID that has performed a LAN Watch using [Monitoring > Assign SNMP](#) (page 276). Click the [SNMP Info](#) hyperlink for the device you're interested in. This displays all MIB object IDs and the SNMP instances available for the device.

- **Value Returned as** - If the MIB object returns a numeric value, you can choose to return this value as a **Total** or a **Rate Per Second**.
2. Optionally change the default MIB object **Name** and **Description**.

## Monitor

3. Select the log data collected. If the returned value is numeric, you can minimize the collection of unwanted log data by setting a collection operator just over or just under the collection threshold.
  - **Collection Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over` or `Under`.
  - **Collection Threshold** - Set a fixed value that the returned value is compare to, using the selected **Collection Operator**, to determine what log data is collected.
  - **SNMP Timeout** - Specify the number of periods the agent waits for a reply from the SNMP device before giving up. Two seconds is the default.
4. Specify when a SNMP alarm condition is triggered.
  - **Alarm Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over`, `Under` or `Percent Of`.
  - **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alarm condition is triggered.
  - **Percent Object** - Selecting the `Percent Of` option for **Alarm Operator** causes this field to display. Enter another object/version/instance in this field whose value can serve as a 100% benchmark for comparison purposes.
  - **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alarm condition. Many alarm conditions are only alarming if the level is sustained over a long period of time.
  - **Ignore additional alarms for** - Suppress additional alarm conditions for this same issue for this time period. This reduces the confusion of many alarm conditions for the same issue.
5. **Warn when within X% of alarm threshold** - Optionally display a warning alarm condition in the **Dashboard List** (page 189) page when the returned value is within a specified percentage of the **Alarm Threshold**. The default warning icon is a yellow traffic light icon . See **SNMP Icons** (page 218).
6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alarm condition will occur.
  - **Trending Activated?** - If yes, a linear regression trendline is calculated based on the last 2500 data points logged.
  - **Trending Window** - The time period used to extend the calculated trendline into the future. If the predicted trendline exceeds the alarm threshold within the future time period specified, a trending alarm condition is generated. Typically a trending window should be set to the amount of time you need to prepare for an alarm condition, if it occurs.
  - **Ignore additional trending alarms for** - Suppresses additional trending alarm conditions for this same issue during this time period.
  - By default, trending alarms display as an orange icon  in the **Dashboard List** (page 189) page. You can change this icon using the **SNMP Icons** (page 218) tab.
  - Warning status alarms and trending status alarms don't create alarm entries in the alarm log, but they change the image of the alarm icon in various display windows. You can generate a trending alarm report using **Reports > Monitor**.

## Next

Moves to the next wizard page.

## Previous

Moves back to the previous wizard page.

## Save

Saves changes to a record.

## Cancel

Ignores changes and returns to the list of records.

## Add SNMP Object

Monitor > Add SNMP Object

Monitor > Define SNMP Set

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center
- Select a SNMP set in a folder, then SNMP Sets > Add Object

When you select objects to include in an SNMP set you're given the opportunity of adding a new SNMP object. This should not be necessary for the most part, because a [LAN Watch](#) (page 272) retrieves the objects you typically require. But if you do need to add an SNMP object from a MIB file manually you can do so using Monitor > [Add SNMP Object](#) (page 217) or by clicking the [Add Object...](#) button while configuring an SNMP set.

The [SNMP MIB Tree](#) page loads a Management Information Base (MIB) file and displays it as an expandable *tree* of MIB objects. All [MIB objects](#) (page 597) are classified by their location on the MIB tree. Once loaded you can select the MIB objects you want to install on your VSA. SNMP device manufacturers typically provide MIB files on their websites for the devices they manufacture.

**Note:** You can review the complete list of MIB objects already installed, by selecting the [MIB OIDs](#) tab in [Monitoring > Monitor Lists](#) (page 202). This is the list of MIB objects you currently can include in an SNMP set.

If a vendor has supplied you with a MIB file, you can follow these steps:

1. Load the vendor's MIB file by clicking [Load MIB ....](#) There may be a message stating there are dependent files that need to be loaded first. The vendor may need to provide those also.
2. Click the  expand icons in the MIB tree—see *the sample graphic below*—and find the desired items to monitor. Select each corresponding check box.
3. Click [Add MIB Objects](#) to move the selected items from Step 2 into the MIB object list.
4. Configure the settings for monitoring the new SNMP object within an SNMP set as you normally would.
5. The number of MIB objects in the tree can soon become unwieldy. Once the desired MIB objects have been added, the MIB file can be removed.

## Load MIB

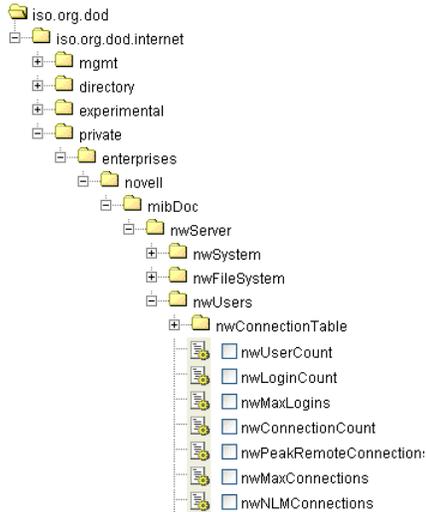
Click [Load MIB...](#) to browse for and upload a MIB file. When a MIB object is added, if the system does not already have the following standard MIB II files—required by most MIBs—it loads them automatically: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Once these files are loaded, the MIB tree located at the bottom of the [Add SNMP Object](#) page can be opened and navigated to find the new objects that the user can select. Most private vendor MIBs are installed under the `Private` folder. See *the sample graphic below*.

**Note:** The MIB file can be loaded and removed at any time and does *not* affect any MIB objects that are used in SNMP sets.

## Monitor

### MIB Tree

The MIB tree represents all MIB file objects that are currently loaded for the user to select from.



### Add MIB Objects

Click [Add MIB Objects](#) to add selected objects to the VSA's list of MIB objects that can be monitored using [Define SNMP Set](#) (*page 213*).

### Remove MIB

After selections have been made the MIB file can be removed. The size of the MIB tree can become so large that it is hard to navigate. Click [Remove MIB](#) to clean that process up.

## SNMP Icons

### Monitor > SNMP Sets

- Select a SNMP set in a folder, then [SNMP Icons](#)

The [SNMP Icons](#) tab selects the SNMP icons that display in the [Dashboard List](#) (*page 189*) page when the following alarm states occur:

- [Select Image for OK Status](#) - The default icon is a green traffic light .
- [Select the Image for Alarm Status](#) - The default icon is a red traffic light .
- [Select Image for Warning Status](#) - The default icon is a yellow traffic light .
- [Select the Image for Trending Status](#) - The default icon is an orange traffic light .
- [Select the Image for Not Deployed Status](#) - The default icon is a grey traffic light .

### Save

Saves changes to a record.

### Upload additional monitoring icons

Select the [Upload additional monitoring icons](#) link to upload your own icons to the status icon drop-down lists.

### Restore

Sets all SNMP icons back to their defaults.

---

# Alerts

## Monitor > Alerts

- This page applies to the following products: *On Premises*, *Kaseya Advanced*, *Kaseya Essentials*, *IT Center*, *IT Workbench*

The **Alerts** page enables you to quickly define alerts for typical **alarm conditions** (page 585) found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the **Low Disk** type of alarm displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alarm immediately to any machine ID displayed on the **Alerts** page and specify the response to the alarm.

**Note:** **Monitor Sets** (page 593) represent a more complex method for monitoring alarm conditions. Typical alarm conditions should be defined using the **Alerts** page.

## Select Alert Function

Select an alert type using the **Select Alert Function** drop-down list.

- **Summary** (page 220)
- **Agent Status** (page 222)
- **Application Changes** (page 225)
- **Get Files** (page 227)
- **Hardware Changes** (page 229)
- **Low Disk** (page 232)
- **Event Logs** (page 234)
- **LAN Watch** (page 240)
- **Agent Procedure Failure** (page 243)
- **Protection Violation** (page 245)
- **New Agent Installed** (page 247)
- **Patch Alert** (page 249)
- **Backup Alert** (page 252)
- **System** (page 256)

## Group Alarms

Alert, system check, and log monitoring alarms are automatically assigned to a **group alarm** category. If an alarm is triggered, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the **Group Alarm Status** (page 194) dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > **Monitor Lists** (page 202). Group alarm column names are assigned to monitor sets using **Define Monitor Set** (page 206).

## Machine Summary Alerts Tab

The **Alerts** tab in the **Machine Summary** page provides, in summary fashion, all the alerts defined for a machine ID. You can use this tab to quickly review, enable, or disable all the alerts applied to a single machine. Typically you display this page by *alt-clicking* the check-in status icon—for example, the  icon—next to any machine ID.

## Reviewing Alarm Conditions with or without Creating Alarms

A user can assign monitor sets, SNMP sets, alerts, system checks or log monitoring to machine IDs *without checking the Create Alarm checkbox* and a **Monitor Action Log** entry will still be created. These logs enable a VSA user to review *alarm conditions* that have occurred with or without being specifically notified by the creation of an alarm, email or ticket. You can generate a report using Info Center > Reports > Monitoring > **Monitor Action Log** (page 167).

## Monitor

### To Create An Alert

The same general procedure applies to all alert types.

1. Select an alert function from the **Select Alert Function** drop-down list.
2. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **Alarm**
  - Create **Ticket**
  - Run **Script**
  - **Email Recipients**
3. Set additional email parameters.
4. Set additional alert-specific parameters. These differ based on the alert function selected.
5. Check the paging rows to apply the alert to.
6. Click the **Apply** button.

### To Cancel an Alert

1. Select one or more paging rows.
2. Click the **Clear** button.

The alert information listed next to the paging row is removed.

## Alerts - Summary

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- **Select Summary** from the **Select Alert Function** drop-down list

The **Alerts - Summary** (page 220) page shows what alerts are enabled for each machine. You can apply or clear settings or copy enabled alerts settings. Specifically you can:

- Apply or clear settings for alarm, ticket and email notification *for all enabled alert types at one time* on selected machines.
- **Copy** all the enabled alert settings from a selected machine ID or machine ID template and apply them to multiple machine IDs.

**Note:** You can only modify or clear alerts initially enabled using the **Copy** option or else by *using the other alerts pages*.

Although you can not assign agent procedures using this page, agent procedure assignments are displayed in the paging area.

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an **alarm condition** (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 189), Monitor > **Alarm Summary** (page 198) and Info Center > Reports > Logs > Alarm Log.

## Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

## Copy

Only active when **Summary** is selected. **Copy** takes all the alert type settings for a single machine ID, selected by clicking **Copy alert settings from <machine\_ID> to all selected machine IDs**, and applies these same settings to all other checked machine IDs.

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Alert Type

Lists all alert types you can assign to a machine ID using the Monitor > **Alerts** (page 219) page. Displays any agent procedure assignments for this machine ID.

## ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **Alarm**
- T = Create **Ticket**

## Monitor

- S = Run Agent Procedure
- E = Email Recipients

## Email Address

A comma separated list of email addresses where notifications are sent. The word `disabled` displays here if no alerts of this alert type are assigned to this machine ID.

## Alerts - Agent Status

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Select Agent Status from the Select Alert Function drop-down list

The **Alerts - Agent Status** (page 222) page triggers an alert when an agent is offline, first goes online, or someone has disabled remote control on the selected machine.

**Note:** When ever the KServer service stops, the system suspends all agent online/offline alerts. If the KServer stops for more than 30 seconds, then agent online/offline alerts are suspended for one hour after the KServer starts up again. Rather than continuously try to connect to the KServer when the KServer is down, agents go to sleep for one hour after first trying to connect a couple times. The one hour alert suspension prevents false agent offline alerts when the KServer starts back up.

## Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Alert when single agent goes off-line
- Alert when users disable remote control
- Alert when agent first goes online - The agent online alert only occurs if an agent offline alert has also been set for the same machine.
- Alert when multiple agents in the same group go off-line - If more than one offline alert is triggered at the same time, email notification is consolidated by group.

**Note:** Changing this email alarm format changes the format for all Agent Status alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<mc>	#mc#	number of machines going offline
<ml>	#ml#	list of multiple machines going offline
<qt>	#qt#	last check-in time
	#subject#	subject text of the email message, if an email was sent in response to an alert

	#body#	body text of the email message, if an email was sent in response to an alert
--	--------	--

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an **alarm condition** (*page 585*) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (*page 189*), Monitor > **Alarm Summary** (*page 198*) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (*page 94*) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (*page 391*).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (*page 600*).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (*page 426*).

### Agent has not checked in for <N> <periods>

If checked, an alert is triggered if the agent has not checked in for the specified number of periods.

### Alert when agent goes online

If checked, an alert is triggered if the agent goes online

### Alert when user disables remote control

If checked, an alert is triggered if the user disables remote control

## Monitor

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

### Email Address

A comma separated list of email addresses where notifications are sent.

### Time Offline

Displays the number of periods a machine ID must be off-line before an alarm condition occurs.

### Rearm Time

The number of periods to ignore additional alarm conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

### Agent Goes Online

Displays a checkmark  if an alert is sent when an agent goes online.

### RC Disabled

Displays a checkmark  if an alert is sent when the user disables remote control.

## Alerts - Application Changes

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Select **Application Changes** from the **Select Alert Function** drop-down list.
- Similar information is provided using **Audit** > **Add/Remove** (page 142) and **Reports** > **Software**.

The **Alerts Application Changes** (page 225) page triggers an alert when a new application is installed or removed on selected machines. You can specify the directories to exclude from triggering an alert. This alert is based on the **latest audit** (page 587).

### Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when application list change

**Note:** Changing this email alarm format changes the format for all **Application Changes** alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<il>	#il#	list of newly installed applications
<rl>	#rl#	list of newly removed applications
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an **alarm condition** (page 585) is encountered, an alarm is created. Alarms are displayed in **Monitor** > **Dashboard List** (page 189), **Monitor** > **Alarm Summary** (page 198) and **Info Center** > **Reports** > **Logs** > **Alarm Log**.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Monitor

### Run Procedure after alert

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

### Alert when audit detects New application installed

If checked, an alert condition is encountered when a new application is installed.

### Alert when audit detects Existing application deleted

If checked, an alert condition is encountered when a new application is removed.

### Exclude directories

You can specify the directories to exclude from triggering an alert. The exclude path may contain the wildcard asterisk (\*) character. Excluding a folder excludes all subfolders. For example, if you exclude `*\windows\*`, `c:\Windows` and all subfolders are excluded. You can add to the current list of applications, replace the current application list or remove the existing application list.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

## Email Address

A comma separated list of email addresses where notifications are sent.

## Installed Apps

Displays a checkmark  if an alert is sent when an application is installed.

## Removed Apps

Displays a checkmark  if an alert is sent when an application is removed.

## (Exclude)

Lists directories excluded from sending an alert when an application is installed or removed.

## Alerts - Get Files

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Select **Get Files** from the **Select Alert Function** drop-down list

The **Alerts - Get File** (page 227) page triggers an alert when a procedure's **Get File** or **Get File in Directory Path** command executes, uploads the file, and the file is now different from the copy previously stored on the KServer. If there was not a previous copy on the KServer, the alarm condition is encountered. Once defined for a machine ID, the same **Get File** alert is *active for any agent procedure* that uses a **Get File** command and is run on that machine ID.

**Note:** The VSA issues the alert only if the **send alert if file changed** option has been selected in the procedure. Turn off alerts for specific files in the agent procedure editor by selecting one of the without alerts options.

## Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when file fetched with **Get File** changes from the last fetch
- Alert when file fetched with **Get File** is unchanged from last fetch

**Note:** Changing this email alarm format changes the format for all **Get Files** alert emails.

## Monitor

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<fn>	#fn#	filename
<gr>	#gr#	group ID
<id>	#id#	machine ID
<sn>	#sn#	procedure name the fetched the file
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Procedure after alert

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.

- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

### Email Address

A comma separated list of email addresses where notifications are sent.

## Alerts - Hardware Changes

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- **Select Hardware Changes** from the **Select Alert Function** drop-down list

The **Alerts - Hardware Changes** (page 229) page triggers an alert when a hardware configuration changes on the selected machines. Detected hardware changes include the addition or removal of RAM, PCI

## Monitor

devices, and disk drives. This alert is based on the [latest audit](#) (page 587).

### Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when disk or PCI card is added or removed
- Alert when the amount of installed RAM changes

**Note:** Changing this email alarm format changes the format for all [Hardware Changes](#) alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<ha>	#ha#	list of hardware additions
<hr>	#hr#	list of hardware removals
<id>	#id#	machine ID
<m>	#m#	new RAM size
<ro>	#ro#	old RAM size
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

## Monitor

### Email Address

A comma separated list of email addresses where notifications are sent.

## Alerts - Low Disk

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Select **Low Disk** from the **Select Alert Function** drop-down list

The **Alerts - Low Disk** (page 232) page triggers an alert when available disk space falls below a specified percentage of free disk space. A subsequent low disk alert is not created unless the target machine's low disk space is corrected, or unless the alert is cleared, then re-applied. This alert is based on the **latest audit** (page 587).

### Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Alert when disk drive free space drops below a set percent

**Note:** Changing this email alarm format changes the format for all **Low Disk** alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<df>	#df#	free disk space
<dl>	#dl#	drive letter
<dt>	#dt#	total disk space
<gr>	#gr#	group ID
<id>	#id#	machine ID
<pf>	#pf#	percent free space
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

## Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

## Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

## Send alert when selected machines have less than <N> % free space on any fixed disk partition

An alert is triggered if a machine's free disk space is less than the specified percentage.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Monitor

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

### Email Address

A comma separated list of email addresses where notifications are sent.

## Alerts - Event Logs

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center
- Select **Event Logs** from the **Select Alert Function** drop-down list

The **Alerts - Event Logs** (page 232) page triggers an alert when an event log entry for a selected machine matches a specified criteria. After selecting the **event log type**, you can filter the alarm conditions specified by **event set** and by **event category**.

**Note:** You can display event logs directly. On a Windows machine click **Start**, then click **Control Panel**, then click **Administrative Tools**, then click **Event Viewer**. Click **Application**, **Security** or **System** to display the events in each log.

### Prerequisite

Event logging must be enabled for a particular machine using Agent > **Event Log Settings** (page 37).

### Windows Event Logs

An **event log service** runs on Windows operating systems (Not available with Win9x). The event log service enables event log messages to be issued by Window based programs and components. These events are stored in event logs located on each machine. The event logs of managed machines can be stored in the KServer database, serve as the basis of alerts and reports, and be archived.

Depending on the operating system, the **event log types** available include but are not limited to:

- Application log
- Security log
- System log
- Directory service log
- File Replication service log
- DNS server log

The list of event types available to select can be updated using Monitoring > **Update Lists by Scan** (page 203).

Windows events are further classified by the following **event log categories**:

- Error
- Warning
- Information
- Success Audit
- Failure Audit
- Critical - Applies only to Vista, Windows 7 and Windows Server 2008
- Verbose - Applies only to Vista, Windows 7 and Windows Server 2008

Event logs are used or referenced by the following VSA pages:

- Monitor > **Agent Logs** (page 34)
- Monitor > Alerts > **Event Logs** (page 234)
- Monitor > Alerts > **Edit Event Sets** (page 239)
- Monitor > **Update Lists by Scan** (page 203)
- Agent > **Log History** (page 35)
- Agent > **Event Log Settings** (page 37)
- Agent > **Agent Logs** (page 34)
- Reports > **Logs** (page 591)
- System > Database Views > **vNtEventLog** (page 497)

## Event Sets

Because the number of events in Windows events logs is enormous the VSA uses a record type called an **event set** to filter an alarm condition.

Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 589) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (\*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

For details on how to configure event sets, see Monitor > Alerts > Event Logs > **Edit Event Sets** (page 239).

## Sample Event Sets

A growing list of sample event sets are provided. The names of sample event sets begin with ZC. You can modify sample event sets, but its better practice to copy a sample event set and customize the copy. Sample event sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.

## Creating an Event Log Alert

1. On the Monitor > **Alerts** page select the **event log type** using the drop-down list.
2. Select the **Event Set** (page 239) filter used to filter the events that trigger alerts. By default <All Events> is selected.
3. Check the box next to any of the following **event category**:
  - Error
  - Warning
  - Information
  - Success Audit
  - Failure Audit
  - Critical - Applies only to Vista, Windows 7 and Windows Server 2008
  - Verbose - Applies only to Vista, Windows 7 and Windows Server 2008

**Note:** Red letters indicate logging disabled. Event logs may be disabled by the VSA for a particular machine, based on settings defined using Agent > Event Log Settings (page 37). A particular event category may not be available for certain machines, such as the Critical and Verbose event categories.

4. Specify the *frequency* of the alarm condition required to trigger an alert:
  - Alert when this event occurs once.
  - Alert when this event occurs <N> times within <N> <periods>.
  - Alert when this event doesn't occur within <N> <periods>.
  - Ignore additional alarms for <N> <periods>.
5. Click the **Add** or **Replace** radio options, then click **Apply** to assign selected event type alerts to selected machine IDs.
6. Click **Remove** to remove all event based alerts from selected machine IDs.

### Global Event Log Black List

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml`. The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

### Flood Detection

If 1000 events—not counting **black list events** (page 590)—are uploaded to the KServer by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your KServer. Alarm detection and processing operates regardless of whether collection is suspended.

### Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Single event log alert. Same template applied to all event log types.
- Multiple event log alerts. Same template applied to all event log types.
- Missing event log alert. Same template applied to all event log types.

**Note:** Changing this email alarm format changes the format for all Event Logs alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<cg>	#cg#	Event category
<cn>	#cn#	computer name
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<ed>	#ed#	event description
<ei>	#ei#	event id

<es>	#es#	event source
<esn>	#esn#	event source name
<et>	#et#	event time
<eu>	#eu#	event user
<ev>	#ev#	event set name
<gr>	#gr#	group ID
<id>	#id#	1. machine ID
<lt>	#lt#	log type (Application, Security, System)
<tp>	#tp#	event type - (Error, Warning, Informational, Success Audit, or Failure Audit)
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

**Note:** Only the following variables can be included in multiple event log alerts: <at> <ed> <ev> <gr> <id> <lt>.

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an **alarm condition** (*page 585*) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (*page 189*), Monitor > **Alarm Summary** (*page 198*) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (*page 94*) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (*page 391*).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (*page 600*).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.

## Monitor

- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## Log Type

The type of event log being monitored.

## ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

## EWISFCV

The event category being monitored.

## Email Address

A comma separated list of email addresses where notifications are sent.

## Event Set

The event set assigned to this machine ID. Multiple events sets can be assigned to the same machine ID.

## Interval

The number of times an event occurs within a specified number of periods. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** option is selected. Displays `Missing` if the **Alert when this event doesn't occur within <N> <periods>** option is selected. Displays `1` if the **Alert when this event occurs once** is selected.

## Duration

The number of periods and event must occur to trigger an alarm condition. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** or **Alert when this event doesn't occur within <N> <periods>** options are selected.

## Re-Arm

Displays the number of periods to wait before triggering any new alarm conditions for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using **Ignore additional alarms for <N> <periods>**.

## Edit Event Sets

**Monitor** > **Alerts** (page 219)

- On the **Alerts** page, select **Event Logs** from the **Select Alert Function** drop-down list.
- Select **<New Event Set>** from the **Define events to match or ignore** drop-down list. The **Edit Event Set** popup window displays.

**Edit Event Sets** filters the triggering of alerts based on the monitoring of events in event logs maintained by the Windows OS of a managed machine. You can assign multiple event sets to a machine ID.

Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 589) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (\*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

**Note:** Normally, if two conditions are added to an event set, they are typically interpreted as an OR statement. If either one is a match, the alert is triggered. The exception is when the **Alert when this event doesn't occur within <N> <periods>** option is selected. In this case the two conditions should be interpreted as an AND statement. Both must *not* happen within the time period specified to trigger an alert.

**Note:** You can display event logs directly. On a Windows machine click **Start**, then click **Control Panel**, then click **Administrative Tools**, then click **Event Viewer**. Click **Application**, **Security** or **System** to display the events in that log. Double-click an event to display its **Properties** window. You can copy and paste text from the **Properties** window of any event into **Edit Event Set** fields.

## To Create a New Event Set

1. On the **Alerts** page, select **Events Logs** from the **Select Alert Function** drop-down list.
2. Select an **Event Log Type** from the second drop-down list.
3. Select **<New Event Set>** from the **Define events to match or ignore** drop-down list. The **Edit Event Set** popup window displays. You can create a new event set by:
  - Entering a new name and clicking the **New** button.
  - Pasting event set data as text.

## Monitor

- Importing event set data from a file.
1. If you enter a new name and click **New**, the **Edit Event Set** window displays the five properties used to filter events.
  2. Click **Add** to add a new event to the event set.
  3. Click **Ignore** to specify an event that should *not* trigger an alarm.
  4. You can optionally **Rename**, **Delete** or **Export Event Set**.

## Ignore Conditions

If an event log entry matches one more more **ignore conditions** in an event set, then no alert is triggered *by any event set*, even if multiple conditions in multiple event sets match an event log entry. Because ignored conditions override *all event sets*, it's a good idea to define just one event set for all ignored conditions, so you only have to look in one place if you suspect an ignored condition is affecting the behavior of all your alerts. You must assign the event set containing an ignored condition to a machine ID for it to override all other event sets applied to that same machine ID.

*Ignore conditions only override events sharing the same log type.* So if you create an "ignore set" for all ignore conditions, it must be applied multiple times to the same machine ID, *one for each log type*. For example, an ignore set applied only as a System log type will not override event conditions applied as Application and Security log type events.

1. On the **Alerts** page, select **Event Logs** from the **Select Alert Function** drop-down list.
2. Check the **Error** checkbox and select `<All Events>` from the event set list. Click the **Apply** button to assign this setting to all selected machine IDs. This tells the system to generate an alert for every error event type. Note the assigned log type.
3. Create and assign an "ignore event set" to these same machine IDs that specifies all the events you wish to ignore. The log type must match the log type in step 2.

## Using the Asterisk (\*) Wildcard

Include an asterisk (\*) wildcard with the text you enter to match multiple records. For example:

```
*yourFilterWord1*yourFilterWord2*
```

This would match and raise an alarm for an event with the following string:

```
"This is a test. yourFilterWord1 as well as yourFilterWord2 are in the description."
```

## Exporting and Importing Edit Events

You can export and import event set records as XML files.

- You can *export* an existing event set record to an XML file using the **Edit Event Set** popup window.
- You can *import* an event set XML file by selecting the `<Import Event Set>` or `<New Event Set>` value from the event set drop-down list.

Example:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<event_sets>
<set_elements setName="Test Monitor Set" eventSetId="82096018">
  <element_data ignore="0" source="*SourceValue*"
    category="*CategoryValue*" eventId="12345"
    username="*UserValue*" description="*DescriptionValue*" />
</set_elements>
</event_sets>
```

## Alerts - LAN Watch

Monitor > Alerts (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center
- Select **LAN Watch** from the **Select Alert Function** drop-down list

The [Alerts - LAN Watch](#) (page 240) page works in conjunction with the [LAN Watch](#) (page 272) page. [LAN Watch](#) scans a machine ID's local LAN and detects new machines and devices connected to the machine's LAN. Both [LAN Watch](#) and the [Alerts - LAN Watch](#) page can subsequently trigger an alert when a new machine or device is discovered on a LAN. Only the [Alerts - LAN Watch](#) page can create a ticket when a new machine or device is discovered on a LAN.

### Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when new device discovered by LAN Watch

Note: Changing this email alarm format changes the format for all [LAN Watch](#) alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<nd>	#nd#	new device data
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Monitor

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

### Email Address

- A comma separated list of email addresses where notifications are sent.

## Alerts - Agent Procedure Failure

Monitor > Alerts (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center
- Select Agent Procedure Failure from the Select Alert Function drop-down list

The Alerts - Agent Procedure Failure (page 243) page triggers an alert when an agent procedure fails to execute on a managed machine. For example, if you specify a file name, directory path or registry key in an agent procedure, then run the agent procedure on a machine ID for which these values are invalid, you can be notified about the agent procedure failure using this alerts page.

### Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:

- Format email message generated by Agent Procedure Failure alerts

Note: Changing this email alarm format changes the format for all Agent Procedure Failure alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<em>	#em#	procedure error message
<en>	#en#	procedure name the fetched the file
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Monitor

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 597):

- A = Create [Alarm](#)

- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

## Email Address

A comma separated list of email addresses where notifications are sent.

## Alerts - Protection Violation

**Monitor** > **Alerts** (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center
- Select Protection Violation from the Select Alert Function drop-down list

The **Alerts - Protection Violation** (page 245) page triggers an alert when a file is changed or access violation detected on a managed machine. Options include **Distributed file changed on agent and was updated**, **File access violation detected**, and **Network access violation detected**.

## Prerequisites

- Agent Procedures > **Distribute File** (page 129)
- Audit > **File Access** (page 85)
- Audit > **Network Access** (page 87)

## Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:

- Format email message generated by Protection Violations alerts.

**Note:** Changing this email alarm format changes the format for all Protection Violation alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<pv>	#pv#	violation description from Agent Log
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

## Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

## Monitor

### Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

### Distributed file changed on agent and was updated

If checked, an alert is triggered when a file distributed using Procedure > [Distributed File](#) (page 129) is changed on the managed machine. The agent verifies the distributed file at every [full check-in](#) (page 588).

### File access violation detected

If checked, an alert is triggered when an attempt is made to access a file specified as blocked using Audit > [File Access](#) (page 85).

### Network access violation detected

If checked, an alert is triggered when an attempt is made to access either an internal or external internet site using an application specified as blocked using Audit > [Network Access](#) (page 87).

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

## Email Address

A comma separated list of email addresses where notifications are sent.

## Alerts - New Agent Installed

[Monitor](#) > [Alerts](#) (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- [Select New Agent Installed](#) from the [Select Alert Function](#) drop-down list

The [Alerts - New Agent Installed](#) (page 247) page triggers an alert when a new agent is installed on a managed machine by selected *machine groups*.

## Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Agent checked in for the first time

**Note:** Changing this email alarm format changes the format for all `New Agent Installed` emails.

The following variables can be included in your formatted email alerts and in procedures.

## Monitor

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<ct>	#ct#	time the agent checked in for the first time
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Machine Group

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

### Email Address

A comma separated list of email addresses where notifications are sent.

## Alerts - Patch Alert

**Patch Management > Patch Alert**

**Monitor > Alerts** (page 219)

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*
- **Select Patch Alert** from the **Select Alert Function** drop-down list.

The **Alerts - Patch Alert** (page 249) page triggers an alert for patch management events on managed machines.

- A new patch is available for the selected machine ID.
- A patch installation failed on the selected machine ID.
- The agent credential is invalid or missing for the selected machine ID.
- Windows Auto Update changed.

### To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **Alarm**
  - Create **Ticket**
  - Run **Script**
  - **Email Recipients**
2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

### To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.
 

The alert information listed next to the machine ID is removed.

### Passing Alert Information to Emails and Procedures

The following types of patch alert emails can be sent and formatted:

- New Patch Available
- Patch Install Failed

## Monitor

- Patch Approval Policies Updated
- Agent Credential Invalid
- Windows Auto Update Configuration Changed

**Note:** Changing the email alarm format changes the format for all **Patch Alert** emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<au>	#au#	auto update change
<bi>	#bi#	bulletin ID
<bl>	#bl#	new bulletin list
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<fi>	#fi#	failed bulletin ID
<gr>	#gr#	group ID
<ic>	#ic#	invalid credential type
<id>	#id#	machine ID
<pl>	#pl#	new patch list
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

### Create Alarm

If checked and an **alarm condition** (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 189), Monitor > **Alarm Summary** (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).

- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Patch Alert Parameters

The system can trigger an alert for the following alarm conditions for a selected machine ID:

- **New patch is available**
- **Patch install fails**
- **Agent credential is invalid or missing**

**Note:** An agent credential (page 588) is not required to install patches unless the machine's File Source (page 340) is configured as Pulled from file server using UNC path. If an agent credential is assigned, it will be validated as a local machine credential without regard to the File Source configuration. If this validation fails, the alert will be raised. If the machine's File Source is configured as Pulled from file server using UNC path, a credential is required. If it is missing, the alert will be raised. If it is not missing, it will be validated as a local machine credential and as a network credential. If either of these validations fails, the alert will be raised.

- **Windows Auto Update changed**

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Monitor

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Approval Policy Updated

Displays as the first row of data. If selected and the [Apply](#) button clicked, an alert is generated when a new patch is added to all patch policies. See [Patch Approval Policy](#) (page 595). This is a system alert and not associated with any machines.

### ATSE

The ATSE response code assigned to machine IDs:

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run Procedure
- E = [Email Recipients](#)

### Email Address

A comma separated list of email addresses where notifications are sent.

### New Patch

If checked, an alarm is triggered when a new patch is available for this machine ID.

### Install Failed

If checked, an alarm is triggered when a patch installation has failed for this machine ID.

### Invalid Credential

If checked, an alarm is triggered when the credential is invalid for this machine ID.

### Win AU Changed

If checked, an alarm is triggered if the group policy for [Windows Automatic Update](#) on the managed machine is changed from the setting specified by Patch Management > [Windows Auto Update](#) (page 335).

**Note:** A log entry in the machine's Configuration Changes log is made regardless of this alert setting.

## Alerts - Backup Alert

[Backup](#) > [Backup Alert](#)

[Monitor](#) > [Alerts](#) (page 219)

- [Select Backup Alert](#) from the [Select Alert Function](#) drop-down list

The [Alerts - Backup Alert](#) (page 252) page triggers an alert for backup events on managed machines.

The list of machine IDs you can select depends on the [machine ID / group ID filter](#) (page 26). To display on this page, machine IDs must have backup software installed on the managed machine using the [Backup > Install/Remove](#) page.

## To Create a Backup Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **A**larm
  - Create **T**icket
  - Run **S**cript
  - **E**mail Recipients
2. Set additional email parameters.
3. Set additional backup alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the **A**pply button.

## To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the **C**lear button.  
The alert information listed next to the machine ID is removed.

## Passing Alert Information to Emails and Procedures

The following types of backup alert emails can be sent and formatted:

- Backup failed
- Verify backup failed
- Recurring backup skipped if machine offline
- Backup Completed Successfully
- Full Backup Completed Successfully
- Image Location free space below

**Note:** Changing the email alarm format changes the format for all Backup Alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<be>	#be#	backup failed error message
<bt>	#bt#	backup type
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<im>	#im#	backup image location
<mf>	#mf#	megabytes free space remaining
<sk>	#sk#	backup skip count

## Monitor

### Create Alarm

If checked and an **alarm condition** (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 189), Monitor > **Alarm Summary** (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Backup Alert Parameters

The system triggers an alarm whenever the system discovers one of four different backup alert conditions for a selected machine ID:

- **Any Backup Completed** - Alerts when any volume or folder backup completes successfully.
- **Full Backup Completed** - Alerts when a full volume or folder backup completes successfully.
- **Backup Fails** - Alerts when a volume or folder backup stops prior to completion for any reason. Typically, backup fails because the machine is turned off mid-backup or because the network connection to the file server referenced by Image Location is lost.
- **Recurring backup skipped if machine offline <N> times** - Alerts when **Skip if machine offline** is set in Schedule Volumes and the backup is rescheduled the specified number of times because the machine is offline. Use this alert to notify you that backups are not even starting because the machine is turned off at the scheduled volume backup time.

- **Image location free space below <N> MB** - Alerts when the hard disk being used to store the backups is less than a specified number of megabytes.

Three additional parameters can be set:

- **Add** - Adds alert parameters to selected machine IDs when **Apply** is selected without clearing existing parameters.
- **Replace** - Replaces alert parameters on selected machine IDs when **Apply** is selected.
- **Remove** - Clear alert parameters from selected machine IDs. Click the edit icon  next to a machine ID group *first* to select the alert parameters you want to clear.

**Note:** You may specify different alert email addresses for each backup alert type. This lets you send backup complete alerts to the user and only send failures to the user.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

**Note:** Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

### Email Address

A comma separated list of email addresses where notifications are sent.

### Any Complete

If checked, an alarm is triggered when any backup is completed for this machine ID.

## Monitor

### Full Complete

If checked, an alarm is triggered when a full backup is completed for this machine ID.

### Backup Fails

If checked, an alarm is triggered when any backup fails for this machine ID.

### Backup Skipped

If checked, an alarm is triggered when any backup is skipped for this machine ID.

## Alerts - System

**Monitor** > [Alerts](#) (page 219)

- This page applies to the following product: **On Premises**
- Select **System** from the [Select Alert Function](#) drop-down list

The [Alerts - System](#) (page 256) page triggers an alert for selected events occurring on the *KServer*. Selecting the [Alerts - System](#) page does not display a managed machine list. The events listed only apply to the *KServer*. This option only displays for **master role users** (page 600).

### Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Admin account disabled manually by another user
- Admin account disabled because logon failed count exceeded threshold
- *KServer* has stopped
- Database backup failed
- Email reader failed ([Ticketing](#) module only)

**Note:** Changing this email alarm format changes the format for all *System* alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<an>	#an#	disabled VSA user name
<at>	#at#	alert time
<bf>	#bf#	database backup error data
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<el>	#el#	email reader error message
<fc>	#fc#	value that tripped the failed logon attempt counter
<fe>	#fe#	time account re-enables
<gr>	#gr#	group ID
<id>	#id#	machine ID
<kn>	#kn#	kserver IP/name
<ms>	#ms#	disabled VSA user type (master or standard)

	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

## Apply

Click [Apply](#) to apply alert parameters to the system.

## Clear

Click [Clear](#) to remove all alert parameters from the system.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

## Admin account disabled

If checked, an alert is triggered when a VSA user account is disabled, whether manually or automatically.

## KServer stopped

If checked, an alert is triggered when the KServer stops.

## System database backup failed

If checked, an alert is triggered when the Kserver's database backup fails

## Email reader in ticketing failed

If checked, an alert is triggered if the Ticketing > [Email Reader](#) (page 449) fails.

## System alerts sent to

Displays the email recipients who are sent system alerts.

---

# SNMP Traps Alert

## Monitor > SNMP Traps Alert

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

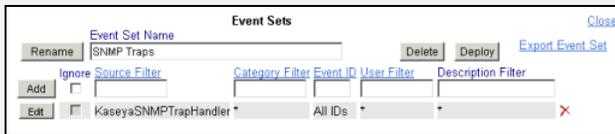
The [SNMP Traps Alert](#) page configures alerts for a managed machine, acting as a SNMP trap "listener",

## Monitor

when it detects an **SNMP trap** message.

When **SNMP Traps Alert** is assigned to a managed machine, a service is started on the managed machine called `Kaseya SNMP Trap Handler`. This service listens for SNMP trap messages sent by SNMP-enabled devices on the same LAN. Each time an SNMP trap message is received by the service, an SNMP trap `Warning` entry is added to the managed machine's `Application` event log. The **source** of these `Application` event log entries is always `KaseyaSNMPTrapHandler`.

**Note:** Create an event set that includes `KaseyaSNMPTrapHandler` as the source. Use asterisks `*` for the other criteria if you don't want to filter the events any more than that.



**Note:** SNMP uses the default UDP port 162 for SNMP trap messages. Ensure this port is open if a firewall is enabled.

## Prerequisite

`Application` event logging with the `warning` event category checked must be enabled for a managed machine using `Agent > Event Log Settings` (page 37).

## Event Sets

Because the number of events in Windows events logs is enormous the VSA uses a record type called an **event set** to filter an alarm condition.

Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 589) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (`*`) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

For details on how to configure event sets, see `Monitor > Alerts > Event Logs > Edit Event Sets` (page 239).

## Creating an SNMP Traps Alert

1. Select the `Monitor > SNMP Traps Alert` page.
2. Select the **Event Set** filter used to filter the events that trigger alerts. Do not select an event set to include *all* SNMP Trap events.
3. Check the box next to the `Warning` **event category**. *No other event categories are used by SNMP Trap Alert.*

**Note:** Red letters indicate logging disabled. Event logs may be disabled by the VSA for a particular machine, based on settings defined using `Agent > Event Log Settings` (page 37).

4. Specify the *frequency* of the alarm condition required to trigger an alert:
  - **Alert when this event occurs once.**
  - **Alert when this event occurs <N> times within <N> <periods>.**
  - **Alert when this event doesn't occur within <N> <periods>.**
  - **Ignore additional alarms for <N> <periods>.**
5. Click the **Add** or **Replace** radio options, then click **Apply** to assign selected event type alerts to selected machine IDs.
6. Click **Remove** to remove all event based alerts from selected machine IDs.
7. Ignore the **SNMP Community** field. *This option is not yet implemented.*

## Passing Alert Information to Emails and Procedures

**Note:** SNMP Traps Alert shares the same Format Email window with Alerts - Event Logs (page 234).

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Create Alarm

If checked and an **alarm condition** (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 189), Monitor > **Alarm Summary** (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online

## Monitor

-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## Log Type

The type of event log being monitored.

## ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

## EWISFCV

The event category being monitored.

## Email Address

A comma separated list of email addresses where notifications are sent.

## Event Set

Displays `All Events` if no *SNMP trap event set* was selected, meaning all SNMP trap events are included.

## Interval

The number of times an event occurs within a specified number of periods. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** option is selected. Displays `Missing` if the **Alert when this event doesn't occur within <N> <periods>** option is selected. Displays `1` if the **Alert when this event occurs once** is selected.

## Duration

The number of periods and event must occur to trigger an alert. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** or **Alert when this event doesn't occur within <N> <periods>** options are selected.

## Re-Arm

Displays the number of periods to wait before triggering any new alerts for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using **Ignore additional alarms for <N> <periods>**.

---

# Assign Monitoring

## Monitor > Assign Monitoring

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Assign Monitoring** page creates monitor set alerts for managed machines. An alert is a response to an alarm condition. An alarm condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

## Monitor Sets

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 596), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Update monitor set counter objects, instances and counters by source machine ID using Monitor > **Update Lists by Scan** (page 203).

**Note:** You must run **Update Lists by Scan** (page 203) for each machine ID you assign a monitor set, to ensure a complete list of monitoring definitions exists on the VSA to monitor that machine.

2. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 202).
3. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 204).
4. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 261).
5. Optionally customize standard monitor sets as *individualized monitor sets*.
6. Optionally customize standard monitor sets using *Auto Learn*.
7. Review monitor set results using:
  - Monitor > **Monitor Log** (page 267)
  - Monitor > **Live Counter** (page 201)
  - Monitor > Dashboard > **Network Status** (page 193)
  - Monitor > Dashboard > **Group Alarm Status** (page 194)
  - Monitor > Dashboard > **Monitoring Set Status** (page 194)
  - Info Center > Reports > Monitor > Monitor Set Report
  - Info Center > Reports > Monitor > Monitor Action Log

**Note:** Changes made to a monitor set affect all machine IDs the monitor set is already assigned to, within a couple minutes of the change.

## Individualized Monitor Sets

You can *individualize* monitor set settings for a single machine.

## Monitor

1. Using Monitor > **Assign Monitoring**, select a *standard* monitor set using the <Select Monitor Set> drop-down list.
2. Assign this standard monitor set to a machine ID. The monitor set name displays in the **Monitor Set** column.
3. Click the individualized monitor set icon  in the **Monitor Set** column to display the same options you see when defining a **standard monitor set** (page 204). *An individualized monitor set adds an (IND) prefix to the name of the monitor set.*
4. Optionally change the name or description of the individualized monitor set, then click the **Save** button. Providing a unique name and description helps identify an individualized monitor set in reports and log files.
5. Make changes to the monitoring settings of the individualized monitor set and click the **Commit** button. Changes apply only to the single machine the individualized monitor set is assigned to.

**Note:** Changes to a standard monitor set have no affect on individualized monitor sets copied from it.

### Auto Learn Alarm Thresholds for Monitor Sets

You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.

To apply **Auto Learn** settings to selected machine IDs:

1. Using Monitor > **Assign Monitoring**, select a *standard* monitor set using the <Select Monitor Set> drop-down list.
2. Click **Auto Learn** to display the **Auto Learn** (page 266) popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard monitor set, modified by your Auto Learn parameters, to selected machine IDs.

**Note:** You cannot apply Auto Learn settings to a monitor set that is already assigned to a machine ID. If necessary, clear the existing assignment of the monitor set to the machine ID, then perform steps 1 through 3 above.

Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

### To Create a Monitor Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **Alarm**
  - Create **Ticket**
  - Run **Script**
  - **Email Recipients**
2. Set additional email parameters.
3. Select the monitor set to add or replace.

4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

### To Cancel a Monitor Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.

The alert information listed next to the machine ID is removed.

### Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

**Note:** Changing this email alarm format changes the format for *all* monitor set and SNMP set emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<ad>	#ad#	alarm duration
<ao>	#ao#	alarm operator
<at>	#at#	alert time
<av>	#av#	alarm threshold
<cg>	#cg#	event category
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<dv>	#dv#	SNMP device name
<gr>	#gr#	group ID
<id>	#id#	machine ID
<ln>	#ln#	monitoring log object name
<lo>	#lo#	monitoring log object type: counter, process, object
<lv>	#lv#	monitoring log value
<mn>	#mn#	monitor set name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

## Monitor

### Create Alarm

If checked and an **alarm condition** (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 189), Monitor > **Alarm Summary** (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

### (Apply Filter)

Enter text in the filter edit box, then click the funnel icon  to apply filtering to the drop-down list displayed in **Select Monitor Set**. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

### Select Monitor Set

Select monitor sets from the **Select Monitor Set** list, then click the **Apply** button to assign the monitor set to selected machine IDs. You may assign more than one monitor set to a machine ID. Add or edit monitor sets using Monitor > **Monitor Sets** (page 204).

**Note:** Sample monitor sets do not display in the **Assign Monitoring** (page 261) > **Select Monitor Set** drop-down list. Create a copy of a sample monitor set by selecting the sample set in **Monitor Sets** (page 204) and clicking the **Save As** button. Your copy of the sample monitor set will display in the drop-down list. In the SaaS version of the VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

### Add Monitor Set

When a monitor set is assigned to machine IDs, the monitor set is added to the list of monitor sets currently assigned to those machine IDs.

## Replace Monitor Set

When a monitor set is assigned to machine IDs, the monitor set replaces all monitor sets already assigned to those machine IDs.

## Apply

Applies the selected monitor set to checked machine IDs.

## Clear

Clears the assignment of a selected monitor set from selected machine IDs.

## Clear All

Clears all monitor sets assigned to selected machine IDs.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Monitor Sets

Displays the list of all monitor sets assigned to machine IDs.



**Edit** - Always displays next to a monitor set. Click this icon to set header parameters to those matching the selected machine ID.



**Override auto learn values** - Displays if Auto Learn is applied to this standard monitor set. Click this icon to display or change the actual values calculated by [Auto Learn](#) (page 266) for this monitor set on this machine ID.



**Individualized monitor set** - Displays if Auto Learn is *not* applied to this standard monitor set. Click this icon to create or make changes to a copy of this [standard monitor set](#) (page 204) that is individualized for this machine ID. *An individualized monitor set adds an (IND) prefix to the name of the monitor set.*

## ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 597):

- A = Create **Alarm**

## Monitor

- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

## Email Address

A comma separated list of email addresses where notifications are sent.

## Auto Learn - Monitor Sets

**Monitor** > **Assign Monitoring** > **Auto Learn**

The **Auto Learn Alarm Thresholds** window maintains auto learn alarm thresholds for monitor sets.

You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.

## Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Edit

A list of **objects/instance/counters** (page 596) displays for the selected monitor set you want to setup to "auto learn". Click the edit icon  to use a wizard that leads you through the three steps required to edit auto learn alarm thresholds.

1. Enable Auto Learn for this object/counter/instance combination, if appropriate, by selecting **Yes - Include**. If **No - Do not include** is selected, no other selections in this wizard are applicable.
  - **Time Span** - Enter the period of time performance data is collected and used to calculate alarm thresholds automatically. Alarms will not be reported during this time period.
2. Displays the **Object**, **Counter** and, if necessary, the counter **Instance** of the alarm threshold being modified. These options cannot be changed.
3. Enter calculated value parameters.
  - **Computation** - Select a calculated value parameter. Options include **MIN**, **MAX** or **AVG**. For example, selecting **MAX** means calculate the maximum value collected by an object/counter/instance during the **Time Span** specified above.
  - **% Increase** - Add this percentage to the **Computation** value calculated above, with the **Computation** value representing 100%. The resulting value represents the alarm threshold.
  - **Minimum** - Set a minimum value for the alarm threshold. The value is automatically calculated as *two standard deviations below* the calculated **Computation** value, but can be manually overridden.
  - **Maximum** - Set a maximum value for the alarm threshold. The value is automatically calculated as *two standard deviations above* the calculated **Computation** value, but can be manually overridden.

**Note:** Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

### Next

Moves to the next wizard page.

### Previous

Moves back to the previous wizard page.

### Save

Saves changes to a record.

### Cancel

Ignores changes and returns to the list of records.

---

## Monitor Log

### Monitor > Monitor Log

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Clicking the monitoring log icon  next to a single alarm for a specific machine ID in the Monitoring Set Status (page 194) dashlet of the Dashboard List page displays this same information as a popup window.

The **Monitor Log** page displays the agent monitoring object logs in chart and table formats.

### Machine ID.Group ID

Click a machine ID link to display log data for all monitor sets assigned to that machine ID. The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404). If no machine IDs display use Monitor > **Assign Monitoring** (page 261) to apply monitor sets to machine IDs.

### Select monitoring object to display information

The page displays a list of monitoring objects assigned to the selected machine ID.

### View

Select a counter object by clicking the **View** link. The selected row is **bolded**. A selected row displays either as a chart or table.

**Note:** If a monitoring object cannot be represented by a chart, only the table view is available.

### Expand Icon

Click the expand icon  to display details about a monitoring object.

### Refresh Data

Click the refresh icon  to refresh data when no values display. Applies to non-responsive monitoring.

## Monitor

If your monitor doesn't show any log values, verify the following:

1. Check the sample interval of the counter object. Once a monitor set is deployed counters return values to the monitor log using their specified sample interval. Wait for the sample interval plus the agent check-in interval for the first value to come back.
2. If there are no values returned, check **Counter Thresholds** (page 208) for the Monitor Counter commands. If no values on the monitored machine or device meet the collection threshold they will not be inserted into the monitor log.

If a monitor isn't responding, the log displays the message `Monitor Not Responding`. There can be several reasons for no response from the monitor:

- **Counters** - If your monitoring set includes a counter that does not exist on a managed machine, the log displays `Not Responding`. You can troubleshoot the monitoring of counters for a specific machine in two ways:
  - Use the Monitor > **Update Lists By Scan** (page 203) page to scan for all monitor counters and services *for that specific machine ID*.
  - Connect to the machine managed by this agent, select the **Run** command in the **Start** menu, enter `perfmon.exe`, click **OK**, create a new **Counter Log**, and check for the existence of the counter objects/counters/instances that aren't responding.
  - A counter value of -998 in the monitor logs indicates the monitor set is returning no data. Check that the `Performance Logs & Alerts` service in Windows is running. This is a pre-requisite for monitoring of performance counters.
- **Services** - If your monitoring set includes a service that does not exist on a managed machine, the log displays `Service Does Not Exist`.
- **Processes** - If your monitoring set includes a process that does not exist on a managed machine, the log displays `Process Stopped`.
- **Permissions** - Make sure that the permissions for the agent's **working directory** (page 78) are set to full access for `SYSTEM` and `NETWORK SERVICE`. This can happen if the agent working directory is placed in the `c:\program files\` or `c:\windows` directories. This is not recommended as these directories have special permissions set by the OS.

### Type

The type of monitor object: counter, process or service.

### Monitor Set Name

The name of the monitor set.

### Object Name

The name of the monitor object.

### Last Value

The last value reported.

### Bar Chart / Table

Select the **Bar Chart** or **Table** radio option to display data in either format. Only monitor objects of type **Counters** can be displayed in bar chart format.

- A bar chart displays the last 2000 data points at the sample interval rate. The background of the chart **displays in red** for alarm threshold, **yellow for warning threshold** and **green for no alarm**.
- Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds. See **Define Monitor Set** (page 213) for more information.

## Select Page

This buttons display only if **Table** format is selected. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

---

# System Check

## Monitor > System Check

- This page applies to the following product: On Premises

The VSA can monitor machines that *don't have an agent installed on them*. This function is performed entirely within a single page called **System Check**. Machines without an agent are called **external systems**. A machine with an agent is assigned the task of performing the system check on the external system. A system check typically determines whether an external system is available or not. Types of system checks include: web server, DNS server, port connection, ping, and custom.

## To Create a System Check Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **Alarm**
  - Create **Ticket**
  - Run **Script**
  - **Email Recipients**
2. Set additional email parameters.
3. Set additional system-check parameters. You may check multiple systems using the same machine ID.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

## To Cancel a System Check Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.
  - The alert information listed next to the machine ID is removed.

## Passing Alert Information to Emails and Procedures

The following types of system check alert emails can be sent and formatted:

- System check alert

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID

## Monitor

<p1>	#p1#	address checked
<p2>	#p2#	additional parameter
<sc>	#sc#	system check type
<scn>	#scn#	system check custom name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

## Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

## Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

## Create Alarm

If checked and an **alarm condition** (*page 585*) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (*page 189*), Monitor > **Alarm Summary** (*page 198*) and Info Center > Reports > Logs > Alarm Log.

## Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (*page 94*) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (*page 391*).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (*page 600*).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (*page 426*).

## System Check Parameters

Select a system check type:

- **Web Server** - Enter a URL to poll at a selected time interval.
- **DNS Server** - Enter a DNS address, either a name or IP, to poll at a selected time interval.

- **Port Connection** - Enter an address, either a name or IP, to connect to, and a port number to connect to, at a selected time interval.
- **Ping** - Enter an address, either a name or IP, to ping at a selected time interval.

**Note:** Do not include the scheme name of a URL in the address you want to ping. For example, do not enter `http://www.google.com`. Instead enter `www.google.com`.

- **Custom** - Enter a path to a custom program and output file to run at a selected time interval.
  - **Program, parameters and output file** - Enter program path. Optionally include a parameter that creates an output file, if applicable. For example: `c:\temp\customcheck.bat > c:\temp\mytest.out`.
  - **Output file path and name** - Enter the name and path of the created output file. For example: `c:\temp\mytest.out`.
  - **Alarm if output file contains / does not contain** - Alarm if output file contains / does not contain the specified text. For example: `Hello World`.

The following optional parameters display for all types of system checks:

- **Every N Period** - Enter the number of times to run this task each time period.
- **Add** - Add this system check to selected machine IDs.
- **Replace** - Add this system check to selected machine IDs and remove all existing system checks.
- **Remove** - Remove this system check from selected machine IDs.
- **Custom Name** - Enter a custom name that displays in alarm messages and formatted emails.
- **Only alarm when service continues to not respond for N periods after first failure detected** - Suppresses the triggering of a system check alarm for a specified number of periods after the initial problem is *detected*, if N is greater than zero. This prevents triggering an alarm for a temporary problem.
- **Ignore additional alarms for N periods** - Suppresses the triggering of additional alarms for the same system check for a specified number of periods after the initial problem is *reported*, if N is greater than zero. This prevents reporting multiple alarms for the same problem.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (*page 583*).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Delete

Click the delete icon  to delete a system check.

## Monitor

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 597):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

### Email Address

A comma separated list of email addresses where notifications are sent.

### Type

The type of system check:

- Web Server
- DNS Server
- Port Connection
- Ping
- Custom

### Interval

The interval for the system check to recur.

### Duration

The number of periods the system check alarm is suppressed, after the initial problem is *detected*. This prevents triggering an alarm for a temporary problem.

### ReArm

The number of periods to ignore additional alarm conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

---

## LAN Watch

Monitor > LAN Watch

Agent > LAN Watch

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

LAN Watch uses an existing VSA **agent** (page 583) on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without agents or **SNMP devices** (page 597). Optionally, the VSA can send an **alert** (page 585) when a LAN Watch discovers any new device. LAN

Watch effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

### Using Multiple Machines on the Same LAN

Typically, you do not have to run a LAN Watch on more than one machine in a scan range. Some reasons to do a LAN Watch on multiple machines within the same scan range include:

- There are multiple SNMP Communities within the same scan range and therefore there are multiple machines with different SNMP Community Read values.
- There are multiple vPro-enabled credentials required.
- There are different alert configurations required.
- The user wishes to have redundant SNMP monitoring.

### Using the Same Operating System for Discovery and Agent Installs

Windows, Macintosh, and Linux agents can discover Windows, Macintosh, and Linux machines on the same LAN using [LAN Watch](#) (page 56). Agent > [Install Agents](#) (page 60) can only install agents on:

- Windows machines if the LAN Watch discovery machine was a Windows machine.
- Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.
- Linux machines if the LAN Watch discovery machine was a Linux machine.

**Note:** Macintosh agent install packages require a credential when using Agent > Install Agent, or when installing agents using the /s "silent install" switch.

**Note:** For Linux machines, the `root` username alone—without a hostname or domain—must be used.

### LAN Watch and SNMP

The LAN Watch discovery machine issues the SNMP requests to the SNMP devices it discovers on the same LAN. So you must run LAN Watch *first* to have access to SNMP-enabled devices using the VSA.

To include SNMP devices in the discovery scan performed by LAN Watch:

1. Select a machine ID on the same LAN as the SNMP devices you want to discover.
2. Specify the IP range to scan using the [Scan IP Range](#) fields. The fields default to the first 1024 IP addresses your selected machine ID belongs to.
3. Check the [Enable SNMP](#) checkbox.
4. Enter a `community` name in the [Read Community Name](#) and [Confirm](#) fields.  
A community name is a credential for gaining access to an SNMP-enabled device. The default "read" community name is typically `public`, in all lower case, but each device may be configured differently. You may have to identify or reset the community name on the device directly if you're not sure what community name to use.
5. Click the [Schedule](#) button, select scheduling parameters, then click the [Submit](#) button. The [Schedule](#) dialog closes.
  - The [Last Scan Started](#) displays the time the LAN Watch started scanning, once it has begun.
  - The [SNMP Active](#) column confirms that SNMP-enabled devices are being scanned as part of the LAN Watch.
6. Review discovered SNMP-enabled devices using the Monitor > Assign SNMP page.

### Schedule

Click [Schedule](#) to display the [Scheduler](#) window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

## Monitor

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

## Cancel

Click **Cancel** to stop the scheduled scan. Cancel also deletes all records of the devices identified on a LAN from the VSA. If you re-schedule LAN Watch after clicking Cancel, each device on the LAN is re-identified as though for the first time.

## Scan IP Range

Set the minimum and maximum IP addresses to scan here. Selecting a machine ID to scan, by checking the box next to that machine's name, automatically fills in the minimum and maximum IP range based on that machine's IP address and subnet mask.

**Note:** LAN Watch does not scan more than 2048 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch limits it to 2048 addresses. LAN Watch only detects addresses on the local subnet to the machine you run LAN Watch from. For example, with a subnet mask of 255.255.255.0, there can be no more than 253 other devices on the local subnet.

## Enable SNMP

If checked, scan for **SNMP devices** (page 597) within the specified **Scan IP Range**.

## Read Community Name / Confirm

LAN Watch can only identify SNMP devices that share the same **SNMP Community** (page 597) *Read* value as the managed machine performing the LAN Watch. Enter the value in the **Read Community Name** and **Confirm** text boxes.

**Note:** Community names are *case sensitive*. Typically the default read community name value is `public`, but may be reset by an administrator to `Public`, `PUBLIC`, etc.

## Enable vPro

Windows only. If checked, identify **vPro** (page 600)-enabled machines within the specified **Scan IP Range**. A machine does not need to be a vPro machine to discover vPro machines using LAN Watch. If a vPro machine is used as the LAN Watch discovery machine, it cannot discover itself.

**Note:** vPro configuration is a prerequisite to using this feature. Refer to the latest Intel documentation for information on how to configure vPro. At the time of this writing, the following link leads to the Intel documentation: <http://communities.intel.com/community/openportit/vproexpert> (<http://communities.intel.com/community/openportit/vproexpert>).

## Username / Password / Confirm

Enter the appropriate vPro credentials to return hardware asset details about vPro machines discovered during the LAN Watch. Typically the same credentials are defined for all vPro machines on the same LAN. The results are displayed using Agent > **View vPro** (page 69).

**Note:** vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using Remote Control > **Power Management** (page 377).

## Enable Alerts

If **Enable Alerts** is checked and a new device is discovered by LAN Watch, an alert is sent to all email addresses listed in **Email Recipients**. LAN Watch alerts and email recipients can also be specified using the Monitor > **Alerts** (page 219) page.

**Note:** Machines that have not been connected to the LAN for more than 7 days and then connect are flagged as new devices and will generate an alert.

## Email Recipients

If alerts are enabled, enter the email addresses where alert notifications are sent. You can specify a different email address for each managed machine, even if it is for the same event. The **From** email address is specified using System > **Outbound Email** (page 426).

## Ignore devices seen in the last <N> days

Enter the number of days to suppress alerts for new devices. This prevents creating alerts for devices that are connected to the network temporarily.

## Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Skip alert if MAC address matches existing agent

Checking this box suppresses alerts if the scan identifies that the MAC address of a network device belongs to an existing managed machine with an agent on it. Otherwise a managed machine that was offline for several days and comes back online triggers an unnecessary alert during a LAN Watch.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## IP Range Scanned

The IP addresses that are scanned by the selected machine ID when LAN Watch runs.

## Monitor

### Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

### Primary DC

Windows only. If a primary domain controller icon  displays, this machine ID is a **primary domain controller** (page 596). If checked, performing a scan on a primary domain controller running Active Directory enables you to "harvest" the users and computers throughout a domain. You can subsequently install VSA agents automatically on computers listed in Active Directory and create VSA users and VSA users based on Active Directory administrator credentials. See **View AD Computers** (page 65) and **View AD Users** (page 66).

### SNMP Active

If the SNMP icon  displays, SNMP devices are included in the scheduled scan.

### vPro Active

Windows only. If the vPro icon  displays, vPro machines are included in the schedule scan.

### Alert Active

If checked  LAN Watch alerts are enabled for this scan.

---

## Assign SNMP

### Monitor > Assign SNMP

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Assign SNMP** page creates SNMP alerts for SNMP devices discovered using a **LAN Watch** (page 272). An **alert** (page 585) is a response to an alarm condition.

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 597). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 597) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 598) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 272).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 276). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 284) or **Dashboard List** (page 189).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 202).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 212).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 217).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 287).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 286).

### Individualized SNMP Sets

You can *individualize* SNMP set settings for a single machine.

1. Select a *standard* SNMP set using the <Select Monitor Set> drop-down list.
2. Assign this standard SNMP set to a SNMP device. The SNMP set name displays in the **SNMP Info / SNMP Set** column.
3. Click the individualized monitor set icon  in the **SNMP Info / SNMP Set** column to display the same options you see when defining a **standard SNMP set** (page 212). *An individualized SNMP set adds an (IND) prefix to the name of the SNMP set.*
4. Make changes to your new individualized SNMP set. These changes apply only to the single SNMP device it is assigned to.

**Note:** Changes to a standard SNMP set have no affect on individualized SNMP sets copied from it.

### Auto Learn Alarm Thresholds for SNMP Sets

You can enable **Auto Learn** alarm thresholds for any standard SNMP set or quick set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis.

Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.

To apply **Auto Learn** settings to selected SNMP devices:

1. Select a *standard* SNMP set using the <Select SNMP Set> drop-down list. Or click the edit icon of an SNMP set already assigned to a device to populate the <Select SNMP Set> drop-down list with its identifier.
2. Click **Auto Learn** to display the **Auto Learn** (page 266) popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard SNMP set, modified by your **Auto Learn** parameters, to selected SNMP devices, if not already assigned.

Once **Auto Learn** is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run **Auto Learn** again, using a new session of actual performance data to re-calculate alarm threshold values.

### Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **LAN Watch** (page 272) is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > **SNMP Sets** and in the drop-down list in Monitor > **Assign SNMP**. A (QS) prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single

## Monitor

device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Monitor > [LAN Watch](#) (page 272).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP](#) (page 276).
3. Click the hyperlink underneath the name of the device, called the [SNMP info](#) (page 281) link, in the [Assign SNMP](#) page to display a dialog.
  - Click [Discovered MIB Objects](#) and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
  - Click [Quick Set Items](#) and, if necessary, edit the alarm thresholds for selected MIB objects.
  - Enter a name after the [\(QS\)](#) prefix in the header of the dialog.
  - Click the [Apply](#) button to apply the quickset to the device.
4. Display SNMP monitoring data returned by the quick set using Monitor > [SNMP Log](#) (page 284), the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > [SNMP Sets](#) (page 598).

### To Create a SNMP Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create [Alarm](#)
  - Create [Ticket](#)
  - Run [Script](#)
  - [Email Recipients](#)
2. Set additional email parameters.
3. Select the SNMP set to add or replace.
4. Check the SNMP device to apply the alert to.
5. Click the [Apply](#) button.

### To Cancel a SNMP Alert

1. Select the SNMP device checkbox.
2. Click the [Clear](#) button.

The alert information listed next to the SNMP device is removed.

### Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

**Note:** Changing this email alarm format changes the format for *all* monitor set and SNMP set emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<ad>	#ad#	alarm duration
<ao>	#ao#	alarm operator
<at>	#at#	alert time
<av>	#av#	alarm threshold

<cg>	#cg#	event category
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<dv>	#dv#	SNMP device name
<gr>	#gr#	group ID
<id>	#id#	machine ID
<ln>	#ln#	monitoring log object name
<lo>	#lo#	monitoring log object type: counter, process, object
<lv>	#lv#	monitoring log value
<mn>	#mn#	monitor set name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

## Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

## Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

## Monitor

### (Apply Filter)

Enter text in the filter edit box, then click the funnel icon  to apply filtering to the drop-down list displayed in [Select SNMP Set](#). Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

### Select SNMP Set

Select SNMP sets from the [Select SNMP Set](#) list, then click the [Apply](#) button to assign the SNMP set to selected machine IDs. You may assign more than one SNMP set to a machine ID. Add or edit SNMP sets using Monitor > [SNMP Sets](#) (page 212).

**Note:** Sample SNMP sets do not display in the [Assign SNMP](#) (page 276) > [Select SNMP Set](#) drop-down list. Create a copy of a sample SNMP set by selecting the sample set in [SNMP Sets](#) (page 212) and clicking the [Save As](#) button. Your copy of the sample SNMP set will display in the drop-down list. In the SaaS version of the VSA, [Save](#) and [Save As](#) buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

### Add Monitor Set

Adds the selected SNMP set to selected SNMP devices.

### Replace Monitor Set(s)

Adds the selected SNMP set to selected SNMP devices and removes all other SNMP sets currently assigned to selected SNMP device.

### Edit SNMP List

Manually add a new SNMP device or edit the information of existing SNMP devices. Enter the IP and MAC address, name and description for the SNMP device. You can also enter the `sysDescr`, `sysLocation` and `sysContact` values typically returned by polling.

### Apply

Applies the selected SNMP set to selected SNMP devices.

### Clear

Clears the assignment of a selected SNMP set from selected SNMP devices.

### Clear All

Clears all SNMP sets assigned to selected SNMP devices.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Name / Type

The name returned by the ARP protocol when a [LAN Watch](#) (page 272) is performed.

### Device IP

The IP address of the SNMP device.

### MAC Address

The MAC address of the SNMP device.

## SNMP Info

Displays the name returned by the SNMP protocol when a LAN Watch is performed. Click the [SNMP Info \(page 281\)](#) link to display the SNMP objects for this SNMP device.

## SNMP Sets

Displays the list of SNMP sets assigned to a SNMP device.



- **Edit** - Always displays next to an SNMP set. Click this icon to set header parameters to those matching the selected SNMP device.



- **Override auto learn values** - Displays if Auto Learn is applied to this standard SNMP set. Click this icon to display or change the actual values calculated by [Auto Learn \(page 266\)](#) for this SNMP set on this SNMP device.



- **Individualized monitor set** - Displays if Auto Learn is *not* applied to this standard SNMP set. Click this icon to create or make changes to a copy of this [standard SNMP set \(page 212\)](#) that is individualized for this SNMP device. *An individualized SNMP set adds an (IND) prefix to the name of the SNMP set.*

## ATSE

The ATSE response code assigned to machine IDs or [SNMP devices \(page 597\)](#):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

## Email Address

A comma separated list of email addresses where notifications are sent.

## SNMP Quick Sets

Monitor > Assign SNMP > [SNMP Info link](#)

The [SNMP Info](#) link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a [LAN Watch \(page 272\)](#) is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > [SNMP Sets](#) and in the drop-down list in Monitor > [Assign SNMP](#). A (QS) prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Monitor > [LAN Watch \(page 272\)](#).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP \(page 276\)](#).
3. Click the hyperlink underneath the name of the device, called the [SNMP info \(page 281\)](#) link, in the [Assign SNMP](#) page to display a dialog.
  - Click [Discovered MIB Objects](#) and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
  - Click [Quick Set Items](#) and, if necessary, edit the alarm thresholds for selected MIB objects.
  - Enter a name after the (QS) prefix in the header of the dialog.
  - Click the [Apply](#) button to apply the quickset to the device.

## Monitor

4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** (page 284), the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > **SNMP Sets** (page 598).

Use the following tabs on the **SNMP Info link** page to configure an SNMP quick set.

### Discovered MIB Objects tab

The **Discovered MIB Objects** tab lists all objects sets discovered by the last SNMP "walk" that apply to the selected SNMP device. You can use this tab to add objects and instances to an SNMP quick set for this device.

- **Add Instance** - Click to add this instance of this object to an SNMP "quick set" displays in the **SNMP Set** tab of this same window.
- **Add All Instances** - Click to add all instances of this object to an SNMP "quick set" displays in the **SNMP Set** tab of this same window.
- **SNMP Object** - The name of the SNMP object. If no name is provided for the object, the OID numerical designation displays.
- **Instance** - The instance of the object. Many objects have multiple instances, each of which have a different value. For example, the different instances could be ports on a router, or paper trays on a printer. The field is blank if the last number of an OID is zero, which indicates there can only be one member of this object. If an instance is not blank, or any number other than 0, than more than one "instance" of this same object exists for the device. You can specify monitoring of multiple instances of an object by entering a range of numbers, such as 1-5, 6 or 1, 3, 7. You can also enter All.
- **Current SNMP Value** - The value returned by the object/instance combination by the latest SNMP "walk".

### Quick Set Items tab

The **Quick Set Items** tab configures the objects and instances selected to be included in your SNMP quick set. Click the edit icon  to define SNMP monitoring attributes for the selected objects. You can also use the **Add** button to add a new object and set these same attributes.

- **SNMP Object** - The SNMP object name or OID number.
- **SNMP Instance** - The last number of an object ID may be expressed as a table of values instead of as a single value. If the instance is a single value, enter 0. If the instance is a table of values, enter a range of numbers, such as 1-5, 6 or 1, 3, 7. You can also enter All.
- **Alarm Operator** - For character string return values, the options are Changed, Equal or NotEqual. For numeric return values, the options are Equal, NotEqual, Over, or Under.
- **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alarm is triggered.
- **Value Returned as** - If the MIB object returns a numeric value, you can choose to return this value as a **Total** or a **Rate Per Second**.
- **Current SNMP Value** - The value returned by the object/instance combination by the latest SNMP "walk".
- SNMP Sets tab

### SNMP Icons tab

- Customize the alarm icons for this *specific SNMP quick set*. See **SNMP Icons** (page 218) for a general explanation of how to use this page.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Commit

Save changes made to this page.

## Cancel

Ignore any changes made to this page and return to the SNMP Sets list.

## Clear

Clears all SNMP objects from all tabs. The default list of objects repopulates the **Discover Objects Set** tab a few minutes later.

## Auto Learn - SNMP Sets

**Monitor** > **Assign SNMP** > **Auto Learn**

The **Auto Learn Alarm Thresholds** window maintains auto learn alarm thresholds for SNMP sets.

You can enable **Auto Learn** alarm thresholds for any standard SNMP set or quick set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis.

Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.

To apply **Auto Learn** settings to selected SNMP devices:

1. Select a *standard* SNMP set using the <Select SNMP Set> drop-down list. Or click the edit icon of an SNMP set already assigned to a device to populate the <Select SNMP Set> drop-down list with its identifier.
2. Click **Auto Learn** to display the **Auto Learn** (page 266) popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard SNMP set, modified by your **Auto Learn** parameters, to selected SNMP devices, if not already assigned.

Once **Auto Learn** is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run **Auto Learn** again, using a new session of actual performance data to re-calculate alarm threshold values.

## Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Edit

Click the edit icon  to use a wizard that leads you through the three steps required to edit auto learn alarm thresholds.

1. Enable Auto Learn for this SNMP object, if appropriate, by selecting *Yes - Include*. If *No - Do not include* is selected, no other selections in this wizard are applicable.
  - **Time Span** - Enter the period of time performance data is collected and used to calculate alarm thresholds automatically. Alarms will not be reported during this time period.
2. Displays the **SNMP Object** of the alarm threshold being modified. This option cannot be changed.

## Monitor

### ➤ Interface

3. Enter calculated value parameters.

- **Computation** - Select a calculated value parameter. Options include `MIN`, `MAX` or `AVG`. For example, selecting `MAX` means calculate the maximum value collected by an SNMP object during the **Time Span** specified above.
- **% Increase** - Add this percentage to the **Computation** value calculated above, with the **Computation** value representing 100%. The resulting value represents the alarm threshold.
- **Minimum** - Set a minimum value for the alarm threshold. The value is automatically calculated as *two standard deviations below* the calculated **Computation** value, but can be manually overridden.
- **Maximum** - Set a maximum value for the alarm threshold. The value is automatically calculated as *two standard deviations above* the calculated **Computation** value, but can be manually overridden.

## Next

Move the user to the next wizard page.

## Previous

Move the user back to the previous wizard page.

## Cancel

Ignore any changes made to wizard pages and return to the **Counter Objects** list.

## Save

Save changes made to the wizard pages.

---

# SNMP Log

## Monitor > SNMP Log

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **SNMP Log** page displays SNMP log data of **MIB objects** (page 597) in a **SNMP Set** (page 212) in chart or table formats.

1. Click a machine ID link to list all SNMP devices associated with a machine ID.
2. Click the IP address or name of an SNMP device to display all SNMP sets and MIB objects assigned to the SNMP device.
3. Click the expand icon  to display the collection and threshold settings for a MIB object.
4. Click the down arrow icon  to display MIB object log data in chart or table formats.
5. Click the **Bar Chart** or **Table** radio options to select the display format for log data.

SNMP monitor objects can contain multiple instances and be viewed together within one chart or table. For example, a network switch may have 12 ports. Each is an instance and can contain log data. All 12 instances can be combined in one chart or table. SNMP bar charts are in 3D format to allow for multiple instance viewing.

## Machine ID.Group ID / SNMP Devices

All machines assigned to SNMP monitoring and currently matching the **Machine ID / Group ID filter** (page 26) are displayed. Clicking the machine ID link displays all SNMP devices associated with the machine ID. Click the SNMP device link to display all MIB objects associated with the SNMP device.

## View

Click the [View](#) link to display log data for a MIB object in a chart or table.

## Remove

Click [Remove](#) to remove log data from a chart or table.

## View All

If the SNMP monitor object has multiple instances, clicking the [View All](#) link displays all data for every instance.

## Remove All

If the SNMP monitor object has multiple instances, clicking the [Remove All](#) link removes all data displayed for each instance.

## Monitor Set Name

The name of the SNMP set the MIB object belongs to.

## Get Object Name

The name of the MIB object used to monitor the SNMP device.

## Description

The description of MIB object in the SNMP set.

## Bar Chart / Table

Select the [Bar Chart](#) or [Table](#) radio button to display data in either format.

- A bar chart displays the last 2000 data points at the sample interval rate. The background of the chart **displays in red** for alarm threshold, **yellow for warning threshold** and **green for no alarm**.
- Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds. See [Define SNMP Set](#) (*page 213*) for more information.

## Display Last

Bar charts display log data for the last number of intervals selected. For example, if you select [Display Last](#) 500 minutes, each bar in the chart represents 1 minute.

## Save View

You can save custom views for each MIB object. The next time this MIB object is selected the saved information is loaded.

## Log rows per Page

These fields only display in [Table](#) format. Select the number of rows to display per page.

## Display Value Over / Under Value

These fields only display in [Table](#) format. Filter the table rows displayed by filtering log data that is over or under the value specified.

## Refresh

Click the refresh button to display the most current log data.

**If your monitor doesn't show any log values**, verify the following.

## Monitor

1. If there are no values returned, check the collection threshold for MIB objects in SNMP sets. If no values on the monitored device meet the collection threshold they are not included in the SNMP log.
2. The log value sample interval is determined by the total number of `SNMPGet` commands retrieving information from SNMP devices to the agent of the machine ID. The more `SNMPGet` commands the larger the sample interval. Check all SNMP devices associated with a machine ID. If some `SNMPGet` commands are returning values but others are not, the `SNMPGet` commands for the failed requests are not compatible.

If a monitor isn't responding, the log displays the message `Monitor Not Responding`. The `SNMPGet` command is incompatible with the device.

---

## Set SNMP Values

### Monitor > Set SNMP Values

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Set SNMP Values](#) page enables you to write values to SNMP network devices. The SNMP objects must be `Read Write` capable and requires entering the Write Community password assigned to the SNMP device.

An SNMP community is a grouping of devices and management stations running SNMP. SNMP information is broadcast to all members of the same community on a network. SNMP default communities are:

- Write = private
- Read = public

**Note:** This page only displays machines that have been previously identified using a [LAN Watch](#) (page 272).

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine ID.Group ID

Lists [Machine ID.Group IDs](#) (page 592) currently matching the [Machine ID / Group ID filter](#) (page 26) and assigned a [SNMP Community](#) (page 597) name. Click a machine ID to display SNMP devices associated with that machine ID.

### SNMP Device

Select the specific SNMP device of interest. This displays a history of `SNMPSet` values written to an SNMP device by the agent of the machine ID.

## Create a SNMPSet command

Click [Create a SNMPSet command](#) to write a new value to this SNMP device. The following fields display:

- **Description** - Enter an easy to remember description of this event. This displays in the history of SNMPSet values for this SNMP device.
- **MIBObject** - Select the MIB object. Click [Add Object](#) (page 217) to add a MIB object that currently does not exist on the [Monitor Lists](#) (page 202) page.
- **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
- **writeCommunity** - The write Community password for the SNMP device. The default write community password is `private`.
- **timeOutValue** - Enter the number of seconds to wait for the SNMP device to respond before the write command times out.
- **setValue** - Enter the value to set the selected MIB object on the SNMP device.
- **attempts** - Enter the number of times to try and write to the MIB object, if it fails to accept the write command.

## Execute SNMPSet

Prepares a procedure that executes a SNMPSet command for the selected SNMP device.

## Cancel

Ignores any data entered and re-displays the [Create a SNMP command](#) link and history.

---

# Set SNMP Type

## Monitor > Set SNMP Type

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center*

The [Set SNMP Type](#) page assigns types to SNMP devices *manually*. SNMP devices assigned to one of these types are monitored by SNMP sets of the same type. You can also give individual SNMP devices custom names and descriptions as well as remove the device from your database.

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value 77 for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a LAN Watch.

**Note:** The entire OID for `system.sysServices.0` is `.1.3.6.1.2.1.1.7.0` or `.iso.org.dod.internet.mgmt.mib-2.system.sysServices.`

You can assign [SNMP sets](#) (page 598) to [devices](#) (page 597) *by type automatically* as follows:

1. Add or edit SNMP *types* using the [SNMP Device](#) tab in Monitor > [Monitor Lists](#) (page 202).
2. Add or edit the value returned by the MIB object `system.sysServices.0` *and associated with each SNMP type* using the [SNMP Services](#) tab in Monitor > [Monitor Lists](#).
3. Associate a SNMP *type* with a SNMP *set* using the [Automatic Deployment to](#) drop-down list in Monitor > SNMP Sets > [Define SNMP Set](#) (page 213).
4. Perform a [LAN Watch](#) (page 272). During the LAN Watch SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a value for the

## Monitor

`system.sysServices.0` MIB object that matches the SNMP type associated with those SNMP sets.

You can also assign **SNMP sets** (page 598) to **devices** (page 597) *manually* as follows:

1. Assign a SNMP type to an SNMP device using Monitor > **Set SNMP Type** (page 287). Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

## Assign

Applies the selected SNMP type to selected SNMP devices.

## Delete

Removes selected SNMP devices from your database. If the device still exists the next time a LAN Watch is performed, the device will be re-added to the database. This is useful if a device's IP or MAC address changes.

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Name

List of SNMP devices generated for the specific machine ID by a **LAN Watch** (page 272).

## Type

The SNMP type assigned to the SNMP device.

## Custom Name

The custom name and custom description assigned to the SNMP device. If a device is given a custom name, the custom name displays instead of the SNMP name and IP address in alarms and in the SNMP log. To change the custom name and description click the edit icon  next to the custom name.

## Device IP

The IP address of the SNMP device.

## MAC Address

The MAC address of the SNMP device.

## SNMP Name

The name of the SNMP device.

---

# Parser Summary

## Monitor > Parser Summary

- This page applies to the following product: On Premises

The **Parser Summary** page displays and optionally define alerts for all parser sets assigned to all machine IDs within the user's scope. **Parser Summary** can also copy parser sets assignments to multiple machine IDs.

**Note:** Copying a parser set to a machine ID on this page *activates* the log parser on the machine IDs it is copied to. Parsing occurs whenever the log file being parsed is updated.

**Note:** You can download a [Configuring Log Parsers Step-by-Step PDF](#) from the first topic of online user assistance.

## Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

## Notification

The agent collects log entries and creates an entry in the log monitoring log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked*. You don't have to be notified each time a new log monitoring entry is created. You can simply [review the Log Monitoring log](#) (page 302) periodically at your convenience.

## To Copy Parser Set Assignments

1. Select a source machine to copy parser set assignments from.
2. Select machine IDs to copy parser set assignments to.
3. Click **Copy**.

## To Create a Parser Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **Alarm**
  - Create **Ticket**
  - Run **Script**
  - **Email Recipients**
2. Set additional email parameters.
3. Check the machine IDs to apply the alert to.
4. Click the **Apply** button.

## To Cancel a Parser Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.

The alert information listed next to the machine ID is removed.

## Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Log Monitoring parser alerts.
- Multiple log monitoring parser alerts.
- Missing log monitoring parser alert.

**Note:** Changing this email alarm format changes the format for both **Assign Parser Sets** and **Parser Summary** emails.

The following variables can be included in your formatted email alerts and in procedures.

## Monitor

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<ec>	#ec#	event count
<ed>	#ed#	event description
<gr>	#gr#	group ID
<id>	#id#	machine ID
<lpm>	#lpm#	Log file set criteria
<lpm>	#lpm#	Log parser set name
<lsn>	#lsn#	Log file set name

## Create Alarm

If checked and an alarm condition (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List (page 189), Monitor > Alarm Summary (page 198) and Info Center > Reports > Logs > Alarm Log.

## Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

## Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 391).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (page 600).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 426).

## Copy

Click **Copy** to copy the parser sets of the machine ID selected using the **this machine ID** link to other machine IDs selected in the paging area.

## Apply

Applies alert checkbox settings to selected machine IDs.

## Clear All

Clears all alert checkbox settings from selected machine IDs.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Delete

Click the delete icon  next to a parser set to delete its assignment to a machine ID.

## Log Set Names

Lists the names of parser sets assigned to this machine ID.

## ATSE

The ATSE response code assigned to machine IDs:

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run Procedure
- E = [Email Recipients](#)

## Email Address

A comma separated list of email addresses where notifications are sent.

## Interval

The interval to wait for the alert event to occur or not occur.

## Duration

Applies only if [Alert when this event occurs <N> times within <N> <periods>](#) is selected. Refers to [<N> <periods>](#).

## Monitor

## Re-Arm

Applies only if **Ignore additional alarms for <N> <periods>** is selected.

---

# Log Parser

## Monitor > Log Parser

- This page applies to the following product: On Premises

The **Log Parser** page defines log parsers and assigns them to selected machine IDs.

**Note:** You can download a *Configuring Log Parsers Step-by-Step PDF* from the first topic of online user assistance.

**Note:** The log parsers are only *active* if they are subsequently assigned a log parser set using **Assign Parser Sets** (page 297).

## Log Monitoring

The VSA is capable of monitoring data collected from many **standard log files** (page 591). **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and **syslog** (page 599) files created for Unix, Linux, and Macintosh operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the KServer database, **Log Monitoring** uses **parser definitions and parser sets** (page 595) to parse each log file and select only the data you're interested in. Parsed messages are displayed in Log Monitoring, which can be accessed using the Agent Logs tab of **Live Connect** (page 380) > Agent Data or the **Machine Summary** (page 137) page or by generating a report using the Agent > Logs - **Log Monitoring** (page 165) page. Users can optionally trigger alerts when a **Log Monitoring** record is generated, as defined using **Assign Parsing Sets** (page 297) or **Parser Summary** (page 288).

## Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

## The Log File Parsing Cycle

The parsing of a log file is triggered whenever the log file is changed. In most cases this involves appending new text to the end of the file. To avoid scanning the entire log file from the beginning each time the file is updated, the agent parses log files as follows:

- After each update the agent stores a "bookmark" of the last 512 bytes of a log file.
- When the log file is updated again, the agent compares the bookmark from the old update with the *same byte position* in the new update.
- Since log files may be archived before the log parser is run, parsing can include archives files if they exist.
- You can specify sets of log files and sets of archive files by specifying full pathnames with asterisk (\*) and question mark (?) wildcards. If a set of files is specified the parser begins with the latest file in the set.
- If the bookmark text is the same in both the old update and the new update, the agent begins parsing text *after the bookmark*.

- If the bookmark text is *not* the same and no Log Archive Path is specified, the agent parses the entire log file from the beginning. If a Log Archive Path is specified, the agent searches for the bookmark in the archive files. If the bookmark cannot be found, the agent bookmarks the end of the log file and starts parsing from there in the next cycle.
- Once parsing is completed a new bookmark is defined based on the last 512 bytes of the newly updated log file and the process repeats itself.

**Note:** The parsing of a log file is not a procedure event itself. Only a new configuration, or reconfiguration, using [Log Parser](#), [Assign Parser Sets](#) or [Parser Summary](#) generates a procedure you can see in the [Procedure History](#) or [Pending Procedure](#) tabs of the [Machine Summary](#) page.

### Apply

Click [Apply](#) to assign a selected log parser to selected machine IDs.

### Clear

Click [Clear](#) to remove a selected log parser from selected machine IDs.

### Clear All

Click [Clear All](#) to remove all log parsers from selected machine IDs.

### New...

Select `<Select Log Parser>` in the [Log File Parser](#) drop-down list and click [New...](#) ([page 293](#)) to create a new log parser.

### Edit...

Select an existing log parser in the [Log File Parser](#) drop-down list and click [Edit...](#) ([page 293](#)) to edit the log parser.

### Add Log Parser / Replace Log Parsers

Select [Add Log Parser](#) to add a log parser to existing machine IDs. Select [Replace Log Parsers](#) to add a log parser and remove all other log parsers from selected machine IDs.

## Log File Parser Definition

[Monitor](#) > [Log Parser](#) > [Log File Parser Definition](#)

The [Log File Parser Definition](#) page defines templates and parameters used to parse log files. Definitions are subsequently assigned to machine IDs using the [Log Parser](#) ([page 292](#)) page. Log parsers are initially private, but can be shared with other users.

### The Log File Parsing Cycle

The parsing of a log file is triggered whenever the log file is changed. In most cases this involves appending new text to the end of the file. To avoid scanning the entire log file from the beginning each time the file is updated, the agent parses log files as follows:

- After each update the agent stores a "bookmark" of the last 512 bytes of a log file.
- When the log file is updated again, the agent compares the bookmark from the old update with the *same byte position* in the new update.
- Since log files may be archived before the log parser is run, parsing can include archives files if they exist.
- You can specify sets of log files and sets of archive files by specifying full pathnames with asterisk (\*) and question mark (?) wildcards. If a set of files is specified the parser begins with the latest file in the set.

## Monitor

- If the bookmark text is the same in both the old update and the new update, the agent begins parsing text *after the bookmark*.
- If the bookmark text is *not* the same and no Log Archive Path is specified, the agent parses the entire log file from the beginning. If a Log Archive Path is specified, the agent searches for the bookmark in the archive files. If the bookmark cannot be found, the agent bookmarks the end of the log file and starts parsing from there in the next cycle.
- Once parsing is completed a new bookmark is defined based on the last 512 bytes of the newly updated log file and the process repeats itself.

**Note:** The parsing of a log file is not a procedure event itself. Only a new configuration, or reconfiguration, using **Log Parser**, **Assign Parser Sets** or **Parser Summary** generates a procedure you can see in the Procedure History or Pending Procedure tabs of the **Machine Summary** page.

## Save

Select **Save** to save changes to a log file parser definition.

## Save As...

Select **Save As...** to save a log file parser definition under a different name.

## Delete

Select **Delete** to delete a log file parser definition.

## Share...

You can share log file parser definitions you own with other **VSA users** (page 397), **user roles** (page 400), or make the procedure public to all users.

## Parser Name

Enter the name of the parser.

## Log File Path

Enter the full UNC pathname or mapped drive pathname on the target machine of the log file you want to parse. You can use asterisk (\*) or question mark (?) wildcards to specify a set of log files. If a log file set is specified, the log parser starts with the latest log file first. Example:

`\\morpheus\logs\message.log` or `c:\logs\message.log`.

## Log Archive Path

Enter the full UNC pathname or mapped drive pathname on the target machine of the archive files you want to parse. You can use asterisk (\*) or question mark (?) wildcards to specify a set of archive files. If an archive set is specified, the log parser starts with the latest log file first. Example: If `message.log` is archived daily to a file in `messageYYYYMMDD.log` format, then you can specify

`c:\logs\message*.log`.

## Description

Enter a description for the log parser.

## Template

The template is used to compare with the log entry in the log file to extract out the required data into parameters. Parameters are enclosed with \$ character in template.

Enter a pattern of text and log file parameters. This pattern is used to search from the beginning of each line in a log file. If a pattern finds a match in the log file, the log file parameters in the pattern are populated with the values extracted from the log file.

You can use a percent (%) wildcard to specify an alphanumeric string of any length. A log file parameter is bracketed with the dollar (\$) symbol. Enter \$\$ to match a pattern of text containing a \$ symbol. Enter %% to match a pattern of text containing a % symbol.

**Note:** Template text patterns are *case sensitive*.

Example:

- **Log text:** 126 Oct 19 2007 12:30:30 127.0.0.1 Device0[123]: return error code -1!
- **Template:** \$EventCode\$ \$Time\$ \$HostComputer\$ \$Dev\$[\$PID\$]:%error code \$ErrorCode\$!
- **Parsed result:**  
EventCode=126  
Time= 2007/10/19 12:30:30 Friday  
HostComputer=127.0.0.1  
Dev=Device0  
PID=123  
ErrorCode=-1

Guidelines:

- To enter a tab character in the template edit box:
  1. Copy and paste a tab character from log data.
  2. Use {tab} if it is enter manually.
- To create a template it is easier to copy the original text into the template, then replace the characters that can be ignored with %. Then replace the characters that are saved to a parameter with a parameter name.
- Make sure all parameters in the template are defined in [Log File Parameters](#).
- A date time parameter must have both date and time information from the source data, otherwise just use a string parameter.

## Multilayer Template

If checked, multiple lines of text and log file parameters are used to parse the log file.

**Note:** The character string {tab} can be used as a tab character and {nl} can be used as a new line break. {nl} cannot be used in single line template. % can be used as wildcard character.

## Output Template

Enter a pattern of text and log file parameters to store in [Log Monitoring](#).

Example:

- **Output template:** Received device error from \$Dev\$ on \$HostComputer\$. Code = \$ErrorCode\$.
- **Result output:** Received device error from Device0 on 127.0.0.1. Code = -1.

## Apply

Click [Apply](#) to add or update a parameter entered in the [Name](#) field.

## Monitor

### Clear All

Click [Clear All](#) to remove all parameters from the parameter list.

## Log File Parameters

### Name

Once the template is created, you need to define the list of parameters used by the template. All the parameters in the template have to be defined, otherwise the parser returns an error. Available parameters are *integer*, *unsigned integer*, *long*, *unsigned long*, *float*, *double*, *datetime*, *string*. The length of parameter name is limited to 32 characters.

Enter the name of a parameter used to store a value. Parameters are subsequently used in the [Template](#) and [Output Template](#) text boxes.

**Note:** Do *not* bracket the name of the parameter with \$ symbols in the Name field. This is only required when the parameter is entered in the [Template](#) and [Output Template](#) text boxes.

### Type

Enter the data type appropriate for the parameter. If data parsed from a log file cannot be stored using that data type, the parameter remains empty.

### Date Format

If the [Type](#) selected is `Date Time`, enter a [Date Format](#).

- `YY, YYYY, YY, YYYY` - two or four digit year
- `M` - single or two digit month
- `MM` - two digit month
- `MMM` - abbreviation of month name, ex. "Jan"
- `MMMM` - full month name, ex. "January"
- `D, d` - single or two digit day
- `DD, dd` - two digit day
- `DDD, ddd` - abbreviation name of day of week, Ex. "Mon"
- `DDDD, dddd` - full name of day of week, ex. "Monday"
- `H, h` - single or two digit hour
- `HH, hh` - two digit hour
- `m` - single or two digit minute
- `mm` - two digit minute
- `s` - single or two digit second
- `ss` - two digit second
- `f` - one or more digit of fraction of second
- `ff` - ffffffff - two to nine digit
- `t` - one character time mark, ex. "a"
- `tt` - two-character time mark, ex. "am"

**Note:** *Date and time filtering in views and reports are based on the log entry time. If you include a `$Time$` parameter using the `Date Time` data type in your template, Log Monitoring uses the time stored in the `$Time$` parameter as the log entry time. If a `$Time$` parameter is *not* included in your template, then the time the entry was added to Log Monitoring serves as the log entry time. Each date time parameter must contain at least the month, day, hour, and second data.*

Example:

- Date time string: `Oct 19 2007 12:30:30`
- DateTime template: `MMM DD YYYY hh:mm:ss`

## UTC Date

**Log Monitoring** stores all date/time values as **universal time, coordinated** (UTC). This enables UTC date and times to be automatically converted to the user's local time when **Log Monitoring** data is displayed or when reports are generated.

If blank, the date and time values stored in the log file parameter are converted from the local time of the machine ID assigned the log parser to UTC. If checked, the date and time values stored in the log file parameter are UTC and no conversion is necessary.

---

# Assign Parser Sets

## Monitor > Assign Parser Sets

- This page applies to the following product: *On Premises*

The **Assign Parser Sets** page creates and edits parser sets and assigns parsers sets to machine IDs. Optionally triggers an alert based on a parser set assignment. A machine ID only displays in the paging area if:

- That machine ID has been previously assigned a **log file parser definition** (*page 293*) using Monitor > **Log Parser** (*page 292*).
- That same log file parser definition is selected in the **Select Log File Parser** drop-down list.

**Note:** *Assigning a parser set to a machine ID on this page **activates** the log parser. Parsing occurs whenever the log file being parsed is updated.*

**Note:** *You can download a **Configuring Log Parsers Step-by-Step PDF** from the first topic of online user assistance.*

## Notification

The agent collects log entries and creates an entry in the log monitoring log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked*. You don't have to be notified each time a new log monitoring entry is created. You can simply **review the Log Monitoring log** (*page 302*) periodically at your convenience.

## Parser Definitions and Parser Sets

When configuring **Log Monitoring** (*page 591*) it's helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A **parser definition** is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in **Log Monitoring**.

## Monitor

A **parser set** subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts.

Without the filtering performed by the parser set, the KServer database would quickly expand. For example a log file parameter called `$FileServerCapacity$` might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in **Log Monitoring**, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

### Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

### To Create a Parser Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **Alarm**
  - Create **Ticket**
  - Run **Script**
  - **Email Recipients**
2. Set additional email parameters.
3. Select the parser set to add or replace.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

### To Cancel a Parser Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.  
The alert information listed next to the machine ID is removed.

### Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Log Monitoring parser alerts.
- Multiple log monitoring parser alerts.
- Missing log monitoring parser alert.

**Note:** Changing this email alarm format changes the format for both **Assign Parser Sets** and **Parser Summary** emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time

<db-view.column>	not available	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<ec>	#ec#	event count
<ed>	#ed#	event description
<gr>	#gr#	group ID
<id>	#id#	machine ID
<lpm>	#lpm#	Log file set criteria
<lpm>	#lpm#	Log parser set name
<lsn>	#lsn#	Log file set name

### Create Alarm

If checked and an [alarm condition](#) (page 585) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 189), Monitor > [Alarm Summary](#) (page 198) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 94) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 391).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for [master role users](#) (page 600).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 426).

### Select Log File Parser

Select a log parser from the [Select log file parser](#) drop-down list to display all machine IDs previously assigned this log parser using the [Log Parser](#) (page 292) page.

### Define log sets to match

After a log parser is selected, click [Edit](#) (page 301) to define a new parser set or select an existing parser set from the [Define log sets to match](#) (page 301) drop-down list.

## Monitor

### Alert when...

Specify the *frequency* of the parser set condition required to trigger an alert:

- [Alert when this event occurs once](#)
- [Alert when this event occurs <N> times within <N> <periods>](#)
- [Alert when this event doesn't occur within <N> <periods>](#)
- [Ignore additional alarms for <N> <periods>](#)

### Add / Replace

Click the [Add](#) or [Replace](#) radio options, then click [Apply](#) to assign a selected parser set to selected machine IDs.

### Remove

Click [Remove](#) to remove all parser sets from selected machine IDs.

### Apply

Applies the selected parser set to checked machine IDs.

### Clear

Clears the assignment of a selected parser set from selected machine IDs.

### Clear All

Clears all parser sets assigned to selected machine IDs.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (*page 583*).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (*page 592*) displayed is based on the [Machine ID / Group ID filter](#) (*page 26*) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (*page 404*).

### Delete

Click the delete icon  next to a parser set to delete its assignment to a machine ID.

## Log Set Names

Lists the names of parser sets assigned to this machine ID.

## ATSE

The ATSE response code assigned to machine IDs:

- A = Create **A**larm
- T = Create **T**icket
- S = Run Procedure
- E = **E**mail Recipients

## Email Address

A comma separated list of email addresses where notifications are sent.

## Interval

The interval to wait for the alert event to occur or not occur.

## Duration

Applies only if **Alert when this event occurs <N> times within <N> <periods>** is selected. Refers to **<N> <periods>**.

## Re-Arm

Applies only if **Ignore additional alarms for <N> <periods> is selected**.

## Log File Set Definition

### Monitor > Assign Parser Sets

- Select a log parser from the **Select log file parser** drop-down list.
- Then select **<New Parser Set>** or an existing parser set from the **Define log set to match** drop-down list. The **Log File Set Definition** popup window displays.

The **Log File Set Definition** page defines parser sets. A parser set is a list of conditions that must be matched to create a **Log Monitoring** record. Each condition combines a parameter, operator and value.

## Parser Definitions and Parser Sets

When configuring **Log Monitoring** (*page 591*) it's helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A **parser definition** is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in **Log Monitoring**.

A **parser set** subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts.

Without the filtering performed by the parser set, the KServer database would quickly expand. For example a log file parameter called `$FileServerCapacity$` might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in **Log Monitoring**, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

### To Create a New Parser Set

1. Enter a name for the parser set.
2. Optionally rename the parser set by entering a new name and click **Rename** to confirm the change.
3. Select a log file parameter from the **Parser Column** drop-down list. Log file parameters are defined using the **Log File Parser Definition** (page 293) this parser set is intended to filter.
4. Select an **Operator** from the drop-down list. Different data types provide different lists of possible operators.
5. Enter the value the log file parameter should have in the **Log File Filter** field to generate a **Log Monitoring** record.

**Note:** Template text patterns are *case sensitive*.

6. Click **Add** to add this parameter/operator/value combination to the list of conditions defined for this parser set.
7. Click **Edit** to edit and then **Save** an existing parameter/operator/value combination.
8. Click the delete icon  to delete an existing parameter/operator/value combination.

---

## Viewing Log Monitoring Entries

Log Monitoring entries are displayed in **Log Monitoring**, which can be accessed using:

- Agents > **Agent Logs** (page 34) > Log Monitoring > (parser definition)
- **Live Connect** (page 380) > Agent Data > Agent Logs > Log Monitoring > (parser definition). Live Connect is displayed by clicking the check-in status icon of a selected machine ID.
- Audit > **Machine Summary** (page 137) > Agent Logs tab > Log Monitoring > (parser definition). The Machine Summary page can also be displayed by *alt-clicking* the check-in status icon of a selected machine ID.
- The Info Center > Reports > Monitor - Logs > Log Monitoring report.

## Chapter 8

# Patch Management

### In This Chapter

Patch Management Overview	305
Scan Machine	310
Patch Status	312
Initial Update	313
Pre/Post Procedure: Patch Management	315
Automatic Update	317
Machine History	318
Machine Update	319
Patch Update	321
Rollback	324
Cancel Updates	325
Create/Delete: Patch Policy	326
Membership: Patch Policy	327
Approval by Policy	329
Approval by Patch	331
KB Override	333
Windows Auto Update	335
Reboot Action	337
File Source	340
Patch Alert	342
Office Source	346
Command Line	348
Patch Location	351

## **Patch Management**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Patch Management Overview

Use the **Patch Management** overview to monitor, scan, install, and verify Microsoft patches on managed machines. Patch management automates the process of keeping all your machines up to date with the latest patches. You decide how and when updates are applied on a per machine basis. See **Methods of Updating Patches** (page 306), **Configuring Patch Management** (page 306), **Patch Processing** (page 307), **Superseded Patches** (page 307), **Update Classification** (page 308) and **Patch Failure** (page 308) for a general description of patch management.

<b>Functions</b>	<b>Description</b>
<b>Scan Machine</b> (page 310)	Determine what patches are missing on managed machines.
<b>Patch Status</b> (page 312)	Display a summary view of installed, missing and denied patches for each managed machine.
<b>Initial Update</b> (page 313)	Perform <i>one-time</i> processing of <i>all</i> approved patches on managed machines.
<b>Pre/Post Procedure</b> (page 315)	Run procedures before and/or after patch Initial Update and Automatic Update.
<b>Automatic Update</b> (page 317)	Update missing approved patches on managed machines automatically on a <i>recurring</i> basis.
<b>Machine History</b> (page 318)	Display a detailed view of patch scan results for each managed machine.
<b>Machine Update</b> (page 319)	Schedule the installation of missing patches for an individual machine.
<b>Patch Update</b> (page 321)	Apply individual patches to multiple machines.
<b>Rollback</b> (page 324)	Uninstall patches from managed machines.
<b>Cancel Updates</b> (page 325)	Cancel pending patch installations.
<b>Create Delete</b> (page 326)	Create and delete machine patch policies.
<b>Membership</b> (page 327)	Assign machine IDs as members of one or more patch policies.
<b>Approval by Policy</b> (page 329)	Approve or deny patches by patch policy.
<b>Approval by Patch</b> (page 331)	Approve or deny patches by patch.
<b>KB Override</b> (page 333)	Override patch policy default approval status by Microsoft knowledge base article.
<b>Windows Auto Update</b> (page 335)	Remotely set the Windows Automatic Updates settings on selected machines.
<b>Reboot Action</b> (page 337)	Determine whether or not to reboot the machine automatically after installing new patches.
<b>File Source</b> (page 340)	Specify where each machine gets new patch installation files from.
<b>Patch Alert</b> (page 342)	Configure alerts for patch-related events, such as when a new patch becomes available for a managed machine.
<b>Office Source</b> (page 346)	Specify an alternate source location for MS Office installation files.
<b>Command Line</b> (page 348)	Set the command line parameters used to install patches.
<b>Patch Location</b> (page 351)	Specify the URL to download a patch from, when the system can not automatically locate it.

## Methods of Updating Patches

The VSA provides **five** methods of applying Microsoft patches to managed machines:

- **Initial Update** is a *one-time* processing of all approved Microsoft patches applicable to a managed machine based on **Patch Policy** (page 595). **Initial Update** ignores the **Reboot Action** (page 337) policy and reboots the managed machine **without warning the user** as often as necessary until the machine has been brought up to the latest patch level. **Initial Update** should only be performed during non-business hours and is typically performed over a weekend on newly added machines.
- **Automatic Update** is the *preferred* method of updating managed machines on a *recurring* basis. Obeys both the **Patch Policy** and the **Reboot Action** policy.
- **Patch Update** - If you're using **Automatic Update**, then **Patch Update** is used on an exception basis to apply individual patches to multiple machines or for patches that originally failed on certain machines. Overrides the **Patch Policy** but obeys the **Reboot Action** policy.
- **Machine Update** - If you're using **Automatic Update**, then **Machine Update** is used on an exception basis to apply patches to individual machines. Overrides the **Patch Policy** but obeys the **Reboot Action** policy. **Machine Update** is often used to test a new patch prior to approving it for general release to all machines.
- **Patch Deploy** - You can also use a user defined procedure to install a Microsoft patch using Agent Procedures > **Patch Deploy** (page 123). Microsoft releases many hot fixes as patches for very specific issues that are not included in the Microsoft Update Catalog or in the Office Detection Tool, the two patch data sources the **Patch Management** module uses to manage patch updates. **Patch Deploy** enables customers to create a patch installation procedure for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

**Note:** You can install non-Microsoft applications using Agent Procedures > **Application Deploy** (page 124). When a pre-defined install solution cannot be used, use Agent Procedures > **Packager** (page 127) to create a self-extracting file ready for automated distribution.

## Configuring Patch Management

### Analyzing Patch Status

You can determine the patch status of managed machines using the following pages:

- Determine what patches are missing on managed machines using **Scan Machine** (page 310).
- Display a summary view of installed, missing and denied patches for each managed machine using **Patch Status** (page 312).
- Display a detailed view of patch scan results for each managed machine using **Patch History** (page 318).

### Configuring Patch Management

Patch Management configuration options directly or indirectly affect the four Patch Management methods of installing patches as follows:

		Initial Update	Automatic Update	Patch Update	Machine Update
<b>Create/Delete</b> (page 326)	Create a <b>patch policy</b> (page 595).				
<b>Membership</b> (page 327)	Assign machine IDs to a patch policy.				
<b>Approval by Policy</b> (page 329)	Set patch approval policies.				
<b>Approval by Patch</b>	Set patch approval policies.				

(page 331)					
<b>KB Override</b> (page 333)	Overrides patch approval policies.	●	●		
<b>Pre/Post Procedure</b> (page 315)	Run procedures before or after <b>Initial Update</b> and <b>Automatic Update</b> .	●	●		
<b>Reboot Action</b> (page 337)	Change the reboot policy for machine IDs.		●	●	●
<b>File Source</b> (page 340)	Change the file source location machines use to download patches.	●	●	●	●
<b>Command Line</b> (page 348)	Change command line parameters for installing selected patches.	●	●	●	●
<b>Patch Location</b> (page 351)	Change the download URL for patches.	●	●	●	●
<b>Patch Alert</b> (page 342)	Configure alerts for patch-related events.	●	●	●	●
<b>Office Source</b> (page 346)	Create an alternate source location for Office patches. A <b>credential</b> (page 83) must be defined to use the <b>Office Source</b> page.	●	●	●	●

**Note:** Windows Auto Update (page 335) enable or disables Windows Auto Update on managed machines regardless of whether patches are installed on machine IDs.

## Patch Processing

When you schedule a patch the following occurs:

1. The agent on the managed machine is told to start the update process at the scheduled time.
2. The patch executable is downloaded to the managed machine from where ever the **File Source** (page 340) is set for that machine ID.
3. The patch file is executed on the managed machine using the parameters specified in **Command Line** (page 348). You should never have to set these switches yourself, but just in case, this capability is there.
4. After all the patches have been installed the managed machine is rebooted. *When* reboots occur for a machine ID depends on the **Reboot Action** (page 337) assigned to that machine ID. Applies to **Machine Update** (page 319), **Patch Update** (page 321) and **Automatic Update** (page 317). Reboots in response to an **Initial Update** (page 313) always occur immediately and without warning the user.
5. The managed machine is rescanned automatically. It takes several minutes after the rescan is complete for this data to show up on the VSA. Wait several minutes before checking the patch state after a reboot.

**Note:** If you schedule multiple patches for installation on the same machine, all the patches are installed at the same time. After all the patches have been installed the machine reboots once. This technique saves time and reboots.

**Note:** Service packs are always installed separately. If you are installing a service pack with other patches you will see a reboot after the service pack install and then another single reboot after all the other patches are installed.

## Superseded Patches

A superseded patch is a patch that doesn't have to be installed because a later patch is available. A typical example is a service pack, which bundles many other patches that have been released before the service pack. If you install the service pack, you don't have to install all the earlier patches.

## Patch Management

**Patch Management** only reports patches superseded by a service pack. Superseded patches have a string appended to the title of the patch that indicates that it is superseded by Service Pack X. This string is displayed as **dark red text with a yellow background** to make it stand out.

Example: **Superseded By: KB936929 Windows XP Service Pack 3 (KB936929)**

The installation process installs superseded updates *only if* the service pack that supersedes these updates *is not* selected for installation. If the superseding service pack is selected for installation, the superseded updates *are not* downloaded or installed. A procedure log entry is added to indicate the update was skipped because it was superseded.

You can deny all superseded patches using the **Override Default Approval Status with Denied for superseded updates in this policy** checkbox in **Approval by Policy** (page 329).

In addition:

- Patch titles in the **Patch Management** (page 169) report include **Superseded By: Service Pack X**, when applicable.
- The patch filter on the patch approval pages now include the ability to filter on **superseded/not superseded**.
- Occasionally, the **Superseded By** warning displays as **Superseded By: Unspecified**. This is typically caused by a cross-operating system patch that is superseded by one or more service packs. This is likely to be seen on updates dealing with Media Player.

## Update Classification

Microsoft updates are organized as follows:

Update Classification	Classification Type (Non-Vista / Vista)	Included in WSUSSCN2.CAB*
Security Updates	High Priority / Important Includes critical, important, moderate, low, and non-rated security updates.	Yes
Critical Updates	High Priority / Important	Yes
Update Rollups	High Priority / Important	Yes
Service Packs	Optional – Software / Recommended	Typically not
Updates	Optional – Software / Recommended	No
Feature Packs	Optional – Software / Recommended	No
Tools	Optional – Software / Recommended	No

In those cases where a machine does not have Internet connectivity at the time of a machine patch scan, Kaseya uses Microsoft's WSUSSCN2.CAB data file. Microsoft publishes this CAB file as needed. It contains a sub-set of the Microsoft Update Catalog. As seen in the table above, scan data for only the high priority updates and occasionally for service packs are included in the CAB file. The KServer automatically downloads the CAB file on a daily basis to make it available for those machines needing this type of scan. See **Windows Automatic Update** (page 600).

## Patch Failure

After the patch installation attempt completes—including the reboot if requested—the system re-scans the target machine. If a patch still shows missing after the re-scan, failure is reported. Patches can fail for several reasons:

- **Insufficient Disk Space** - Patches are downloaded, or copied from a file share, to the local machine's hard disk. Several patches, especially service packs, may require significant additional local disk space to completely install. Verify the target machine has plenty of disk space available.

- **Bad Patch File** - The phrase `Bad Patch File` in the **Comments** column indicates the patch file failed to execute for some reason. If you schedule multiple patches to install as a batch and even *one* of them fails, all the patches are marked as `Bad Patch File`. The system is reporting a procedure failure and can not distinguish which patch in the procedure caused the failure.
- **Corrupted Patch File** - The downloaded patch file is corrupt.
- **Missing Patch Location** - The phrase `Missing patch location` in the **Comments** column means the URL used to download patches from the Microsoft website is missing. You can manually enter the correct location using the **Patch Location** (page 351) page.
- **No Reboot** - Several patches require a system reboot before they take effect. If your **Reboot Action** (page 337) settings did not allow a reboot, the patch may be installed but will not be effective until after the reboot.
- **Command Line Failed** - If the command line parameters set in the **Command Line** (page 348) function are incorrect, the patch executable typically displays a dialog box on the managed machine stating there is a command line problem. This error causes patch installation to halt and the patch installation procedure to terminate. The patch file remains on the managed machine and `Install Failed` is displayed. Enter the correct command line parameters for the patch and try again.

**Note:** Command line parameters for each patch apply globally and can only be changed by a master role user.

- **MS Office Command Line Failed** - The only command line parameter permitted for use with Microsoft Office (prior to Office 2007) related patches is `/Q`. Because MS Office (prior to Office 2007) patches may require the Office installation CD(s), the use of the `/Q` command line parameter might cause the patch install to fail. If an Office related patch fails, remove the `/Q` command line parameter and try again.

**Warning:** The only switch permitted for use with Microsoft Office 2000, XP, and 2003 related patches (marked as Office) is `/Q`. If `/Q` is not specified, Microsoft Office 2000, XP, and 2003 switches will be reset to `/INSTALL-AS-USER`. Microsoft Office 2003 patches may also include the `/MSOCACHE` switch used to attempt a silent install if the `MSOCache` exists on the machine and the `/INSTALL-AS-USER` switch is set.

- **Patch Download Blocked** - The patch file was never delivered to the machine. The system downloads the patch directly from the internet to either the KServer, a file share, or directly to the managed machine, depending on the machine ID's **File Source** (page 340) settings. The machine ID's firewall may be blocking these downloads. A patch file delivered to the agent with a size of only 1k or 2k bytes is an indication of this problem.
- **User not logged in** - In some cases a user on the machine being patched must be logged in to respond to dialogs presented by the install during the patch. The patch procedure automatically detects whether a user is currently logged in and will not continue if a user is not logged in. Reschedule the installation of the patch when a user is available and logged in to the machine.
- **Credential does not have administrator rights** - If a credential is defined for a machine ID, then **Patch Management** installs all new patches using this credential. Therefore, **Set Credential** (page 83) should always be a *user with administrator rights*.
- **Manual install only** - Not a patch failure, but a requirement. Some patches and service packs require passwords or knowledge of a customized setup that the VSA can not know. The VSA does not automatically install patches having the following warnings:

```
Manual install only
Patch only available from Windows Update web site
No patch available; must be upgraded to latest version
```

These updates must be installed manually on each machine.

### Troubleshooting Patch Installation Failures

When patch scan processing reports patch installations have failed, a `KBxxxxxxx.log` (if available) and the `WindowsUpdate.log` are uploaded to the KServer. Additionally, for those patches that required an "Internet based install", a `ptchdlin.xml` file will be uploaded to the KServer. These files can be reviewed using Agent Procedures > [Get File](#) (page 127) for a specific machine and can help you troubleshoot patch installation failures. Info Center > Reports > Logs > Agent Procedure Log contains entries indicating these log files have been uploaded to the KServer for each machine.

---

## Scan Machine

### Patch Management > Scan Machine

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Scan Machine](#) page schedules scans to search for missing patches on each managed machine. Scanning takes very little resources and can be safely scheduled to run at any time of day. The scanning operation does not impact users at all.

### Scanning Frequency

System and network security depends on all your machines having the latest security patches applied. Microsoft typically releases patches on Tuesdays. Security and critical patches are typically released on the second Tuesday of the month (Patch Tuesday), and non-security and non-critical patches are typically released on the third and/or fourth Tuesdays of the month, but these schedules are not guaranteed. To ensure your machines are updated you should scan all managed machines on a daily basis.

### Scanning the KServer

To scan the KServer, you must install an agent on the KServer. Once installed, you can scan the KServer just like any other managed machine.

### View Definitions

You can filter the display of machine IDs on any agent page using the following options in [View Definitions](#) (page 28).

- [Machines that have no patch scan results \(unscanned\)](#)
- [Last execution status for patch scan success / failed](#)
- [Patch scan schedule / not schedule](#)
- [Patch scan has / has not executed in the last <N> <periods>](#)

### Remind me when machines need a patch scan scheduled

If checked, a warning message displays the number of machine IDs not currently scheduled. The number of machine IDs reported depends on the [Machine ID / Group ID filter](#) (page 26) and machine groups the user is authorized to see using System > [Scope](#) (page 404).

### Schedule

Click [Schedule](#) to display the [Scheduler](#) window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

- [Distribution Window](#) - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.

- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

### Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

### Run Now

Click **Run Now** to run this task on selected machine IDs immediately.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (*page 583*).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (*page 592*) displayed is based on the **Machine ID / Group ID filter** (*page 26*) and the machine groups the user is authorized to see using System > User Security > **Scopes** (*page 404*).

### Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

### Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

This timestamp shows the next scheduled scan. Overdue date/time stamps display as **red text with yellow highlight**.

### Recurrence

If recurring, displays the interval to wait before running the task again.

---

## Patch Status

### Patch > Patch Status

- This page applies to the following products: *On Premises*, *Kaseya Advanced*, *Kaseya Essentials*, *IT Center*, *IT Workbench*
- Similar information is provided using *Info Center > Reports > Patch Management* (page 169).

The **Patch Status** page provides a summary view of the patch status for each of your managed machines. You can quickly identify machines that are missing patches or are indicating errors. The total of all missing patches is the sum of the **Missing Approved**, **Missing Denied**, and **Missing Manual**.

### Patch Test

Most patch problems are the result of configuration and/or permission issues. The test function exercises the entire patch deployment process without actually installing anything on the target machine or causing a reboot. If a machine ID's operating system does not support patching, the operating system is displayed. Each count in the paging area is hyperlinked. Clicking a count's hyperlink displays a list of all patches that make up that count.

- The system resets test results every time a machine ID's **File Source** (page 340) or **Set Credential** (page 83) changes.
- Test cancels any pending patch installs *except Initial Updates* (page 313).
- Machines being processed by **Initial Update** are *not* tested. The **Initial Update** status message and date/time is displayed instead of the column totals.

### View Definitions

You can filter the display of machine IDs on any agent page using the following options in **View Definitions** (page 28).

- **Machines with Patch Test Result**
- **Machines missing greater than or equal to N patches**
- **Use Patch Policy**

### Test

Click **Test** to verify patches can update selected machine IDs. Does not actually install any patches.

### Cancel

Click **Cancel** to stop the test.

### Auto Refresh Table

If checked, the paging area is automatically updated every five seconds. This checkbox is automatically selected and activated whenever **Test** is clicked.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes

- Agent is currently offline
- Agent has never checked in
- 🚫 Agent is online but remote control has been disabled
- 🛑 The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Install Patches

The number of patches installed.

### Missing Approved

The number of approved patches missing.

### Missing Denied

The number of unapproved patches missing.

### Missing Manual

The number of approved patches missing that must be installed manually. These patches cannot be processed by **Automatic Update** (page 317), **Initial Update** (page 313), **Machine Update** (page 319), or **Patch Update** (page 321).

### Pending Patches

The number of patches scheduled to be installed.

### User Not Ready

The number of patches not installed because the patch requires:

- the user to be logged in, or
- the user to take action and the user declined or did not respond.

### Failed Patches

The number of patches that attempted to install but failed.

### Test Results

The status returned after clicking the **Test** button:

- Untested
- Pending
- Passed
- Failed

---

## Initial Update

### Patch Management > Initial Update

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

**Initial Update** is a *one-time* processing of all approved Microsoft patches applicable to a managed machine based on **Patch Policy** (page 595). **Initial Update** ignores the **Reboot Action** (page 337) policy and

## Patch Management

reboots the managed machine **without warning the user** as often as necessary until the machine has been brought up to the latest patch level. **Initial Update** should only be performed during non-business hours and is typically performed over a weekend on newly added machines. See **Methods of Updating Patches** (page 306), **Configuring Patch Management** (page 306), **Patch Processing** (page 307), **Superseded Patches** (page 307), **Update Classification** (page 308) and **Patch Failure** (page 308) for a general description of patch management.

**Note:** The agent for the KServer is not displayed on this page. **Initial Update** cannot be used on the KServer.

## Patch Update Order

Service packs and patches are installed in the following order:

1. Windows Installer
2. OS related service packs
3. OS update rollups
4. OS critical updates
5. OS non-critical updates
6. OS security updates
7. Office service packs
8. Office update rollups
9. All remaining Office updates

**Note:** Reboots are forced after each service pack and at the end of each patch group **without warning**. This is necessary to permit the re-scan and installation of the subsequent groups of patches.

## Pre/Post Procedures

Agent procedures can be configured to be executed just before an **Initial Update** or **Automatic Update** begins and/or after completion. For example, you can run agent procedures to automate the preparation and setup of newly added machines before or after **Initial Update**. Use Patch Management > **Pre/Post Procedures** (page 315) to select and assign these agent procedures on a per-machine basis.

## Schedule

Click **Schedule** to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule this task *once*. Options include:

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.

## Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.

-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

**Note:** Displays the following message if applicable: Not a member of a Patch Policy - All missing patches will be installed!

## Scheduled

This timestamp shows the scheduled **Initial Update**.

## Updated

If checked, an **Initial Update** has been performed successfully on the machine ID. The timestamp shows when the **Status** being reported was completed.

## Status

During processing, the **Status** column displays the following types of messages, if applicable:

- Started
- Processing Windows Installer
- Processing operating system service packs
- Processing operating system update rollups
- Processing operating system critical updates
- Processing operating system non-critical updates
- Processing operating system security updates
- Processing Office service packs
- Processing Office update rollups
- Processing Office updates

When all processing has been completed, the **Status** column displays either:

- Completed - fully patched
- Completed - remaining patches require manual processing

If the latter status displays, select the appropriate machine ID in Patch Management > **Machine Update** (page 319) to determine why all patches were not applied. Some patches might require manual install or for the user to be logged in. In the case of patch failures, manually schedule failed patches to be reapplied. Due to occasional conflicts between patches resulting from not rebooting after each individual patch, simply reapplying the patches typically resolves the failures.

---

# Pre/Post Procedure: Patch Management

## Patch Management > Pre/Post Procedure

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

Use the **Pre/Post Procedure** page to run procedures either before and/or after **Initial Update** (page 313) or

**Automatic Update** (page 317). For example, you can run procedures to automate the preparation and setup of newly added machines before or after **Initial Update**.

**Note:** Post procedures run even if there are patch installation failures.

### To Run a Pre/Post Procedure

1. Select machine IDs or **machine ID templates** (page 592) in the paging area.
2. Check one or more of the following checkboxes and select an agent procedure for each checkbox you check:
  - Run select agent procedure before Initial Update
  - Run select agent procedure after Initial Update
  - Run select agent procedure before Automatic Update
  - Run select agent procedure after Automatic Update
3. Click **Set**.

### Skip Auto Update

The **Auto Pre-Agent Procedure** can be used to determine whether the **Automatic Update** should be executed or not. After executing the **Auto Pre-Agent Procedure**, a registry value is checked on the machine. If this registry value exists **Automatic Update** is skipped; otherwise, **Automatic Update** is executed. To invoke this feature, the **Auto Pre-Agent Procedure** must include a procedure step to set the registry value below:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Kaseya\Agent\SkipAutoUpdate
```

**Note:** Any data type and any data value may be set. The test is for existence only.

If this registry value exists, a procedure log entry is made to document that **Automatic Update** was skipped, and this registry key is deleted.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Init Pre-Agent Procedure / Init Post-Agent Procedure

This column lists the procedures set to run before and/or after an [Initial Update](#).

## Auto Pre-Agent Procedure / Auto Post-Agent Procedure

This column lists the procedures set to run before and/or after an [Automatic Update](#).

---

# Automatic Update

## Patch Management > Automatic Update

- This page applies to the following products: [On Premises](#), [Kaseya Advanced](#), [Kaseya Essentials](#), [IT Center](#)

The [Automatic Update](#) page is the *preferred* method of updating managed machines with Microsoft patches on a *recurring* basis. [Automatic Update](#) obeys both the [Patch Approval Policy](#) (page 595) and the [Reboot Action](#) (page 337) policy. Use [Initial Update](#) (page 313) if you are installing patches for the first time on a managed machine. See [Methods of Updating Patches](#) (page 306), [Configuring Patch Management](#) (page 306), [Patch Processing](#) (page 307), [Superseded Patches](#) (page 307), [Update Classification](#) (page 308) and [Patch Failure](#) (page 308) for a general description of patch management.

- Patches that require manual intervention are not included in [Automatic Updates](#). These are shown in the [Missing Manual](#) column of the [Patch Status](#) (page 312) page and on the individual [Machine Update](#) (page 319) page.
- Patch installation only occurs when a new missing patch is found by [Scan Machine](#) (page 310).
- [Automatic Update](#) is suspended for a machine while [Initial Update](#) is being processed. [Automatic Update](#) automatically resumes when [Initial Update](#) completes.

## Schedule

Click [Schedule](#) to display the [Scheduler](#) window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

- [Distribution Window](#) - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- [Skip if offline](#) - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- [Power up if offline](#) - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- [Exclude the following time range](#) - If checked, specifies a date/time range to *not* perform the task.

## Cancel

Click [Cancel](#) to cancel execution of this task on selected managed machines.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Patch Management

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

**Note:** Displays the following message if applicable: Not a member of a Patch Policy - All missing patches will be installed!

### Recurrence

If recurring, displays the interval to wait before running the task again.

---

## Machine History

### Patch Management > Machine History

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*
- Similar information is provided using [Info Center > Reports > Patch Management](#) (page 169) and the [Patch Status](#) tab of the [Machine Summary](#) (page 137) and [Live Connect](#) (page 380) pages.

The [Machine History](#) page displays the results from the most recent patch scan of managed machines. All [installed](#) and [missing](#) patches applicable to a managed machine are listed, regardless of whether the patch is approved or not.

- Click a machine ID link to display its patch history.
- Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.
- Patches classified as security updates have a security bulletin ID (MSYY-xxx). Clicking this link displays the security bulletin.
- The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is *Common Windows Component*. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

### Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 307) for more information.

### (Patch)

Patches are grouped by update classification first and knowledge base article number second.

## (Status)

The following status messages can appear next to a patch:

- Installed (date unknown)
- Installed (<datetime>)
- Missing
- Denied by Patch Approval
- Denied (Pending Patch Approval)
- Manual install to VSA database server only - Applies to SQL Server patches on the database server where the KServer database is hosted
- Manual install to KServer only - Applies to Office or any "install-as-user" patches on the KServer
- Patch Location Pending - Applies to patches with an invalid patch location. See [Invalid Patch Location Notification](#) in System > [Configure](#) (page 412).
- Missing Patch Location
- Ignore

---

# Machine Update

## Patch Management > Machine Update

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*
- Similar information is provided using [Info Center > Reports > Patch Management](#) (page 169) and the Patch Status tab of the [Machine Summary](#) (page 137) and [Live Connect](#) (page 380) pages.

The [Machine Update](#) page manually installs Microsoft patches on individual machines. [Machine Update](#) overrides the [Patch Approval Policy](#) (page 595) but obeys the [Reboot Action](#) (page 337) policy. If you're using [Automatic Update](#), then [Machine Update](#) is used on an exception basis. [Machine Update](#) is often used to test a new patch prior to approving it for general release to all machines. See [Methods of Updating Patches](#) (page 306), [Configuring Patch Management](#) (page 306), [Patch Processing](#) (page 307), [Superseded Patches](#) (page 307), [Update Classification](#) (page 308) and [Patch Failure](#) (page 308) for a general description of patch management.

## Using Machine Update

1. Click a machine ID to display all patches missing on that machine.
2. The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.
3. Optionally click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.
4. Optionally click a [Security Bulletin](#) link to review a security bulletin, if available. Patches classified as security updates have a security bulletin ID (`MSyy-xxx`).
5. Check the box next to patches you want installed on the selected machine ID.
6. Click the [Schedule](#) button to install patches using the install parameters.
7. Click the [Cancel](#) button to remove any pending patch installs.

## Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 307) for more information.

## Patch Management

### Schedule

Click this button to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule this task *once*. Options include:

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

### Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

**Note:** Patches that are currently being processed (status of Pending - Processing Now) cannot be cancelled.

### Hide patches denied by Patch Approval

If checked, hides patches denied patch approval. Patches with the status `Pending Approval` are considered denied by **Machine Update**.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### (Patch)

Patches are grouped by update classification first and knowledge base article number second.

### (Status)

The following status messages can appear next to a patch:

- Pending (Processing Now)
- Pending (Scheduled to run at <date>)
- Install Failed - See **Patch Failure** (page 308).
- Awaiting Reboot
- User not logged in
- User not ready to install
- Install Failed - Missing Network Credential
- Install Failed - Invalid Network Credential or LAN Server Unavailable
- Install Failed - Invalid Credential
- Missing
- Denied by Patch Approval
- Denied (Pending Patch Approval)
- Manual install to database server only - Applies to SQL Server patches on the database server where the KServer database is hosted
- Manual install to KServer only - Applies to Office or any "install-as-user" patches on the KServer

- Patch Location Pending - Applies to patches with an invalid patch location. See [Invalid Patch Location Notification](#) in System > [Configure](#) (page 412).
- Missing Patch Location
- Ignore

---

## Patch Update

### Patch Management > Patch Update

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Patch Update](#) page updates missing Microsoft patches on all machines displayed in the paging area. [Patch Update](#) overrides the [Patch Approval Policy](#) (page 329) but obeys the [Reboot Action](#) (page 337) policy. If you're using [Automatic Update](#), then [Patch Update](#) is used on an exception basis to apply individual patches to multiple machines or to re-apply patches that originally failed on certain machines. See [Methods of Updating Patches](#) (page 306), [Configuring Patch Management](#) (page 306), [Patch Processing](#) (page 307), [Superseded Patches](#) (page 307), [Update Classification](#) (page 308) and [Patch Failure](#) (page 308) for a general description of patch management.

### Patches Displayed

The display of patches on this page are based on:

- The [Machine ID/Group ID filter](#) (page 592).
- The patches reported using [Scan Machine](#) (page 310). Managed machines should be scanned daily.
- The patches of machines using [Automatic Update](#) (page 317). If the [Hide machines set for Automatic Update](#) box is checked, these patches are *not* listed here. These patches are automatically applied at the [Automatic Update](#) scheduled time for each machine.
- If the [Hide patches denied by Patch Approval](#) box is checked, patches that are denied or pending approval are not listed here.
- The patches of machines being processed by [Initial Update](#) (page 313). These patches are excluded from this page until [Initial Update](#) completes.

### Duplicate Entries

Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. [Patch Update](#) displays patches sorted by [Update Classification](#) or [Product](#) first and knowledge base article number second. Check the [Product](#) name or click the [KB Article](#) link to distinguish patches associated with a common knowledge base article.

### Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 307) for more information.

### Using Patch Update

1. Optionally click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.
2. Patches classified as security updates have a security bulletin ID (MSYY-xxx). Optionally click the [Security Bulletin](#) link to review the security bulletin, if available.
3. Optionally click the box next to a [KB Article](#) to schedule that patch on all managed machines missing that patch.
4. Optionally click the [Machines...](#) button to schedule a patch on individual machines or to set machines to ignore a patch. The [Ignore](#) setting applies to the selected patch on the selected

## Patch Management

machines. If **Ignore** is set, the patch is considered *Denied*. Patches marked as **Ignore** on the selected machines cannot be installed by any of the installation methods. To be installed, the **Ignore** setting must be cleared.

**Note:** A warning icon  indicates the patch status for one or more machines should be checked before installing this patch. Click the **Machines** button and review the **Status** column for each machine missing this patch.

5. Click the **Schedule** button to install the patches using the install parameters.
6. Click the **Cancel** button to remove any pending patch installs.

### Hide machines set for Automatic Update

If checked, hides patches missing from machine IDs set to **Automatic Update** (page 317).

### Hide patches denied by Approval Policy

If checked, hides patches denied by **Patch Approval Policy** (page 595).

### Patch Group By

Display patch groups by **Classification** or **Product**.

### Schedule

Click this button to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule this task *once*. Options include:

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

### Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

**Note:** Patches that are currently being processed (status of *Pending - Processing Now*) cannot be cancelled.

### Show Details

Click the **Show Details** checkbox to display the expanded title and installation warnings, if any, of each patch.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Status Warning Icon

A warning icon  indicates the patch status for one or more machines should be checked before installing this patch. Click the **Machines** button and review the **Status** column for each machine missing this patch.

## Machines...

Click [Machines...](#) to list all machines missing this patch. On the details page, the following status messages can appear next to a patch:

- Pending (Processing Now)
- Pending (Scheduled to run at <date>)
- Install Failed - See [Patch Failure](#) (page 308).
- Awaiting Reboot
- User not logged in
- User not ready to install
- Install Failed - Missing Network Credential
- Install Failed - Invalid Network Credential or LAN Server Unavailable
- Install Failed - Invalid Credential
- Missing
- Denied by Patch Approval
- Denied (Pending Patch Approval)
- Manual install to database server only - Applies to SQL Server patches on the database server where the KServer database is hosted
- Manual install to KServer only - Applies to Office or any "install-as-user" patches on the KServer
- Patch Location Pending - Applies to patches with an invalid patch location. See [Invalid Patch Location Notification](#) in System > [Configure](#) (page 412).
- Missing Patch Location
- Ignore

## KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

## Security Bulletin

Patches classified as security updates have a security bulletin ID (MSYY-xxx). Clicking this link displays the security bulletin.

## Missing

The number of machines missing this patch.

## Auto

Displays only if the [Hide machines set for Automatic Update](#) box is *not* checked. The number of machines scheduled to install this patch by [Automatic Update](#).

## Ignore

The number of machine set to ignore a patch using the [Machines](#) button. The [Ignore](#) setting applies to the selected patch on the selected machines. If [Ignore](#) is set, the patch is considered `Denied`. Patches marked as [Ignore](#) on the selected machines cannot be installed by any of the installation methods. To be installed, the [Ignore](#) setting must be cleared.

### Product

The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

### Update Classification

See [Update Classification](#) (page 308) for an explanation of **Classification** and **Type**.

---

## Rollback

### Patch Management > Rollback

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Rollback** page removes patches after they have been installed on a system. Not all patches may be uninstalled. The system only lists patches supporting the rollback feature.

**Warning:** Removing Windows software in the wrong order (<http://support.microsoft.com/kb/823836/>) may cause the operating system to stop functioning.

### To Remove a Patch from a Managed Machine

1. Click the machine ID that you want to remove a patch from.
2. Check the box to the left of the patch you want to uninstall.
3. Click the **Rollback** button.

### Rollback

Click this button to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule this task *once*. Options include:

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
- **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- **Exclude the following time range** - If checked, specifies a date/time range to *not* perform the task.

### Cancel

Click **Cancel** to clear a scheduled rollback.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### (Patch)

Patches are grouped by update classification first and knowledge base article number second.

## KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

## Security Bulletin

The security bulletin associated with a patch. Patches classified as security updates have a security bulletin ID (MSYY-xxx). Click the [Security Bulletin](#) link to review the security bulletin, if available.

## (Product)

The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

## (Install Date)

Includes the date the patch was installed, if available.

---

# Cancel Updates

## Patch Management > Cancel Updates

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Cancel Updates](#) page clears *all manually scheduled* patch installations on selected machine IDs.

The [Cancel Updates](#) page can also *terminate* currently running patch installation processes. A [Terminate](#) button displays next to the machine name when a patch installation is being processed. Termination deletes existing patch installation procedures for the selected machine, and the installation process ends after the currently running procedure completes.

**Note:** Remove patches from managed machines using [Rollback](#) (page 324).

**Note:** Use the [Initial Updates](#) (page 313) page to cancel a scheduled [Initial Update](#) or to cancel an [Initial Update](#) that is currently being processed.

**Note:** Use the [Automatic Update](#) (page 317) page to cancel a scheduled [Automatic Update](#).

## Cancel

Click [Cancel](#) to clear all scheduled patch installations scheduled by either [Machine Update](#) or by [Patch Update](#) on selected machine IDs.

## View By

View patches sorted by `machine` or by `patch` first.

## Show patch list

If [View By](#) `machine` is selected and [Show patch list](#) is checked, all *scheduled patch IDs* for each machine ID are listed. If [Show patch list](#) is blank, the *total number of scheduled patches* are listed for each machine ID.

## Patch Management

### Show machine list

If [View By patch](#) is selected and [Show machine list](#) is checked, all *scheduled patch IDs* for each machine ID are listed. If [Show machine list](#) is blank, the *total number of scheduled patches* are listed for each machine ID.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

---

## Create/Delete: Patch Policy

### Patch Management > Patch Policy: Create/Delete

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Create/Delete](#) page creates or deletes patch policies. Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.

- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- [Initial Update](#) (page 313) and [Automatic Update](#) (page 317) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 329) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 331) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 333) overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- [Patch Update](#) (page 321) and [Machine Update](#) (page 319) can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

### Create

Click [Create](#) to define a new patch policy, after entering a new machine patch policy name in the edit field.

### Delete

Click [Delete](#) to delete selected patch policies.

### Enter name for a new patch policy

Enter the name for a new patch policy.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Edit Icon

Click the edit icon  to the left of a patch policy to rename it.

### Policy Name

Lists all machine patch policies defined for the entire system.

### Member Count

Lists the number of machines that are members of each patch policy.

### Show Members

Click [Show Members](#) to list the members of a patch policy.

---

## Membership: Patch Policy

[Patch Management](#) > [Patch Policy: Membership](#)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Membership](#) page assigns machine IDs to one or more patch policies. Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be

## Patch Management

members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- **Initial Update** (page 313) and **Automatic Update** (page 317) require patches be approved before these patches are installed.
- **Approval by Policy** (page 329) approves or denies patch by *policy*.
- **Approval by Patch** (page 331) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- **KB Override** (page 333) overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- **Patch Update** (page 321) and **Machine Update** (page 319) can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

### View Definitions

You can filter the display of machine IDs on any agent page using the following options in **View Definitions** (page 28).

- **Show/Hide members of patch policy**
- **Use Patch Policy**

### Assign machines to a patch policy

Click one or more patch policy names to mark them for adding or removing from selected machine IDs.

### Add

Click **Add** to add selected machine IDs to selected patch policies.

### Remove

Click **Remove** to remove selected machine IDs from selected patch policies.

### Always show all Patch Policies to All Users

If checked, always show all patch policies to all users. This allows all non-master role users to deploy patch policies, even if they did not create the patch policies and don't have machines yet that use them. If blank, only master role users can see all patch policies. If blank, non-master role users can only see patch policies assigned to machines within their scope or to unassigned patch policies they created. This option only displays for **master role users** (page 600).

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Policy Membership

Displays a comma separated list of patch policies that each machine ID is a member of.

---

# Approval by Policy

## Patch Management > Approval by Policy

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Approval by Policy** page approves or denies the installation of Microsoft patches on managed machines by *patch policy*. Patches pending approval are considered denied until they are approved. This gives you the chance to test and verify a patch in your environment before the patch automatically pushes out. See **Methods of Updating Patches** (page 306), **Configuring Patch Management** (page 306), **Patch Processing** (page 307), **Superseded Patches** (page 307), **Update Classification** (page 308) and **Patch Failure** (page 308) for a general description of patch management.

## Setting Patch Approval Policies

Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- **Initial Update** (page 313) and **Automatic Update** (page 317) require patches be approved before these patches are installed.
- **Approval by Policy** (page 329) approves or denies patch by *policy*.
- **Approval by Patch** (page 331) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- **KB Override** (page 333) overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- **Patch Update** (page 321) and **Machine Update** (page 319) can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

## Superseded Patches

A patch may be superseded and not need to be installed. See **Superseded Patches** (page 307) for more information.

## Policy

Select a patch policy by name from the drop-down list.

## Save As...

Click **Save As...** to save the currently selected patch policy to a new policy with identical settings. All patch approval/denial statuses are copied as are the default approval statuses for the policy. Machine membership is *not* copied to the new policy.

### Copy Approval Statuses to Policy <Policy> / Copy Now

Select a policy to copy approval statuses *to*, from the currently selected policy. Then click **Copy Now**. This enables you to perform patch testing against a group of test machines using a test policy. Once testing has been completed and the patches have been approved or denied, use the copy feature to copy only the approved or denied statuses from the test policy to a production policy.

### Policy View / Group By

Display patch groups by classification or product.

### Patch Approval Policy Status

This table displays the approval status of patches by update classification or product group. **Approved**, **Denied**, **Pending Approval**, and **Totals** statistics are provided for each update classification or product group.

Select a **Default Approval Status** for any category for this patch policy. Newly identified patches for this patch policy are automatically set to this default value. Choices include:

-  - Approved
-  - Denied
-  - Pending Approval

**Note:** If the same patch is assigned two different **Default Approval Status** settings—one by update classification *and* the other by product group—then the more restrictive of the two defaults has precedence: Denied over Pending Approval over Approved.

Click any link in this table to display a **Patch Approval Policy Details** page listing individual patches and their approval status. The list is filtered by the type of link clicked:

- **Classification** or **Product**
- **Approved**
- **Denied**
- **Pending Approval**
- **Totals**

In the **Patch Approval Policy Details** page you can:

- Approve or deny approval of patches individually.
- Click the **KB Article** link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

**Note:** Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. Check the **Product** name or click the **KB Article** link to distinguish patches associated with a common knowledge base article.

- Click the **Security Bulletin** link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSYY-xxx).
- The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.
- See **Update Classification** (page 308) for an explanation of **Classification** and **Type**.
- Click the **Show Details** checkbox to display the expanded title, patch status notes and installation warnings, if any, of each patch.

- Click [Filter...](#) to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.
- Optionally add a note, up to 500 characters, using [Patch Status Notes](#). The note is added when the [Approve](#) or [Deny](#) buttons are selected. If the text box is empty when the [Approve](#) or [Deny](#) buttons are selected, the note is removed for selected patches.

### Override Default Approval Status with Denied for "Manual Install Only" updates in this policy

If checked, all existing and future `Manual Install Only` updates are set to denied for this policy.

### Override Default Approval Status with Denied for "Windows Update Web Site" updates in this policy

If checked, all existing and future `Windows Update Web Site` updates are set to denied for this policy.

### Override Default Approval Status with Denied for superseded updates in this policy

If checked, all existing and future superseded patches are set to denied for this policy.

**Note:** Checking an override checkbox has a *one-time effect* on *existing* patches for that category of patches. If you approve an *existing* patch belonging to an override category *after* checking its override checkbox, the patch will remain approved regardless of any override setting. Future patches will continue to default to denied.

---

## Approval by Patch

### Patch Management > Approval by Patch

- This page applies to the following products: `On Premises`, `Kaseya Advanced`, `Kaseya Essentials`, `IT Center`

The [Approval by Patch](#) page approves or denies the installation of Microsoft patches on managed machines by `patch` for *all* patch policies. Changes affect patches installed by all users. This saves you the trouble of approving pending patches separately for each patch policy. See [Methods of Updating Patches](#) (page 306), [Configuring Patch Management](#) (page 306), [Patch Processing](#) (page 307), [Superseded Patches](#) (page 307), [Update Classification](#) (page 308) and [Patch Failure](#) (page 308) for a general description of patch management.

### Setting Patch Approval Policies

Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.

## Patch Management

- **Initial Update** (page 313) and **Automatic Update** (page 317) require patches be approved before these patches are installed.
- **Approval by Policy** (page 329) approves or denies patch by *policy*.
- **Approval by Patch** (page 331) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- **KB Override** (page 333) overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- **Patch Update** (page 321) and **Machine Update** (page 319) can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

## Superseded Patches

A patch may be superseded and not need to be installed. See **Superseded Patches** (page 307) for more information.

## Patch Data Filter Bar

You can filter the data displayed by specifying values in each field of the **Patch Data Filter Bar** at the top of the page.



The screenshot shows a horizontal filter bar with three text input fields labeled 'KB Article: \*', 'Classification: \*', and 'Product: \*'. To the right of these fields is a magnifying glass icon and the word 'Apply'. Further right is a dropdown menu labeled 'Patch View: kadmin Patch View' with a downward arrow. To the right of the dropdown are two buttons: 'Edit...' with a pencil icon and 'Reset' with a trash can icon.

Enter or select values in the **KB Article**, **Classification** or **Products** fields. You can also click the **Edit...** button to filter by additional fields and save the filtering selections you make as a view. Supports **advanced filtering** (page 30) logic. Saved views can be shared using the **Make Public (others can view)** checkbox when editing the view.

## Patch Status Notes

Optionally add a note, up to 500 characters, using **Patch Status Notes**. The note is added when the **Approve** or **Deny** buttons are selected. If the text box is empty when the **Approval** or **Deny** buttons are selected, the note is removed for selected patches.

## Approve

Click **Approve** to approve selected patches for all patch policies.

## Deny

Click **Deny** to deny selected patches for all patch policies.

## Show Details

Check **Show Details** to display multiple rows of information for all patches. This includes the title of a patch, the number of patch policies that have been approved, denied, or are pending approval for a patch, patch status notes, and installation warnings, if any.

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## KB Article

Click the **KB Article** link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

**Note:** Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. Check the **Product** name or click the **KB Article** link to distinguish patches associated with a common knowledge base article.

## Security Bulletin

Click the **Security Bulletin** link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSyy-xxx).

## Product

The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

## Classification / Type

See **Update Classification** (page 308) for an explanation of **Classification** and **Type**.

## Approval Status

The approval status for this patch in *all* policies. Displays `Mixed` if even 1 policy differs from all other policies. Clicking the **Approval Status** link displays a page displaying the approval status assigned to this patch by each policy.

## Published

The date the patch was released.

## Language

The language the patch applies to.

---

# KB Override

## Patch Management > KB Override

- This page applies to the following products: `On Premises`, `Kaseya Advanced`, `Kaseya Essentials`, `IT Center`

The **KB Override** page sets overrides of the *default* approval status of patches set using **Approval by Policy** (page 329) by **KB Article** for *all* patch policies. It also sets the approval status for *existing* patches by **KB Article** for all patch policies. Changes affect patches in *all* patch policies installed by *all* users. See **Methods of Updating Patches** (page 306), **Configuring Patch Management** (page 306), **Patch Processing** (page 307), **Superseded Patches** (page 307), **Update Classification** (page 308) and **Patch Failure** (page 308) for a general description of patch management.

For example, KB890830, "The Microsoft Windows Malicious Software Removal Tool" is released monthly. If you decide to approve all patches associated with this KB Article using KB Override, then not only are existing patches approved but all *new* patches associated with this KB article are automatically approved each month the new patch is released.

## Setting Patch Approval Policies

Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your

## Patch Management

workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- **Initial Update** (page 313) and **Automatic Update** (page 317) require patches be approved before these patches are installed.
- **Approval by Policy** (page 329) approves or denies patch by *policy*.
- **Approval by Patch** (page 331) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- **KB Override** (page 333) overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- **Patch Update** (page 321) and **Machine Update** (page 319) can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

## KB Article

Enter the KB Article number to approve or deny. Do not include the KB prefix.

**Note:** See [Approval by Policy](#) (page 329) or [Approval by Patch](#) (page 331) for a listing of all available KB Articles.

## Override Notes

Enter a note to remind VSA users why the override was set.

## Approve

Click **Approve** to approve patches associated with this KB Article. Multiple patches can be associated with a KB Article.

## Deny

Click **Deny** to deny patches associated with this KB Article. Multiple patches can be associated with a KB Article.

## KB Article

Click the **KB Article** link to display the KB article.

## Override Status

Approved or Denied. Applies to all patches associated with this KB Article.

## Admin

The user who approved or denied patches associated with this KB Article.

## Changed

The date and time the user approved or denied patched associated with this KB Article.

## Notes

Reminds VSA users why the override was set.

---

# Windows Auto Update

## Patch > Windows Auto Update

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The [Windows Auto Update](#) page determines whether [Windows Automatic Updates](#) on managed machines is disabled, left for the user to control, or configured.

## Windows Automatic Updates

Windows Automatic Updates is a Microsoft tool that automatically delivers updates to a computer. Windows Automatic Updates is supported in the following operating systems: Windows 2003, Windows XP, Windows 2000 SP3 or later, and all operating systems released after these. Patch Management > [Windows Auto Update](#) (*page 335*) can enable or disable this feature on managed machines. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems can.

## Windows Automatic Update Cannot Use Template Accounts

Windows Automatic Updates is one feature that cannot be preconfigured in a [machine ID template](#) (*page 592*). This is because Windows Automatic Updates is only supported on Windows 2000 SP3/SP4, Windows XP, Windows Server 2003, and later operating systems. Since a machine ID template cannot specify an operating system, a setting for this feature cannot be stored in the machine ID template. Also, a machine's current settings must be known before they can be overridden. The current settings are obtained when a [Scan Machine](#) (*page 310*) is performed.

**Note:** A checkbox does not display for any machine that either has an operating system that does not support Windows Automatic Updates or for which an initial [Scan Machine](#) has not been completed.

## View Definitions

You can filter the display of machine IDs on any agent page using the [Machines with Patch Automatic Update configuration](#) option in [View Definitions](#) (*page 28*).

## Apply

Click [Apply](#) to apply parameters to selected machine IDs.

## Disable

Select [Disable](#) to disable Windows Automatic Updates on selected machine IDs and let [Patch Management](#) control patching of the managed machine. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user *cannot* change any of the settings. Users can still patch their systems manually.

## User Control

Let machine users enable or disable Windows Automatic Updates for selected machine IDs.

## Configure

Forces the configuration of Windows Automatic Updates on selected machine IDs to the following settings. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user *cannot* change any of the settings. Users can still patch their systems manually.

## Patch Management

- **Notify user for download and installation** - Notifies the user when new patches are available but does not download or install them.
- **Automatically download and notify user for installation** - Automatically downloads updates for the user but lets the user choose when to install them.
- **Automatically download and schedule installation** - Automatically downloads updates and installs the updates at the scheduled time.

### Schedule every day / <day of week> at <time of day>

Applies only if **Automatically download and schedule installation** is selected. Perform this task every day or once a week at the specified time of day.

### Force auto-reboot if user is logged on

Optionally check the box next to **Force auto-reboot if user is logged on**. By default, **Windows Auto Update** does *not* force a reboot. **Reboot Action** (page 337) settings do not apply to **Windows Auto Update**.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Machine Updated

Displays the status of configuring Windows Automatic Updates on selected machine IDs using this page.

- Pending - Windows Automatic Updates is being configured on the selected machine ID.
- Timestamp - The date and time Windows Automatic Updates was configured on the selected machine ID.

### Windows Automatic Update Configuration

The Windows Automatic Update configuration assigned to each selected machine ID.

**Note:** If the **Windows Automatic Update Configuration** column displays `Automatic Update not initialized on machine`, the user must select the **Windows Automatic Updates** icon in the system tray to run the **Windows Automatic Updates Setup** wizard to setup **Windows Automatic Updates**. This is sometimes required on older operating systems.

---

# Reboot Action

## Patch Management > Reboot Action

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Reboot Action** page defines how reboots are performed after a patch install. Patch installs do not take effect until after a machine is rebooted. The **Reboot Action** policy applies to **Machine Update** (page 319), **Patch Update** (page 321) and **Automatic Update** (page 317). It does *not* apply to **Initial Update** (page 313). See **Methods of Updating Patches** (page 306), **Configuring Patch Management** (page 306), **Patch Processing** (page 307), **Superseded Patches** (page 307), **Update Classification** (page 308) and **Patch Failure** (page 308) for a general description of patch management.

**Warning:** It is strongly recommended that the **Reboot Action** for agents installed on the KServer and the database server used by the KServer be set to `Do not reboot after update`. Automatic rebooting of the KServer or database server can have adverse effects on other KServer processes!

## Patch Process

The patch installation procedure runs at the scheduled time and performs the following steps:

- Downloads, or copies from a file share, all the patch files to a local drive, typically the same drive the agent is installed on.
- Executes each patch file, one at a time.
- Performs a reboot of the machine, as specified by this page.

**Note:** If you schedule multiple patches for installation on the same machine, all the patches are installed at the same time. After all the patches have been installed the machine reboots once. This technique saves time and reboots.

**Note:** Service packs are always installed separately. If you are installing a service pack with other patches you will see a reboot after the service pack install and then another single reboot after all the other patches are installed.

## View Definitions

You can filter the display of machine IDs on any agent page using the following options in **View Definitions** (page 28).

- **Show machines that have/have not rebooted in the last N periods**
- **Machines with Reboot Pending for patch installations**

## Apply

Click **Apply** to apply parameters to selected machine IDs.

## Reboot immediately after update.

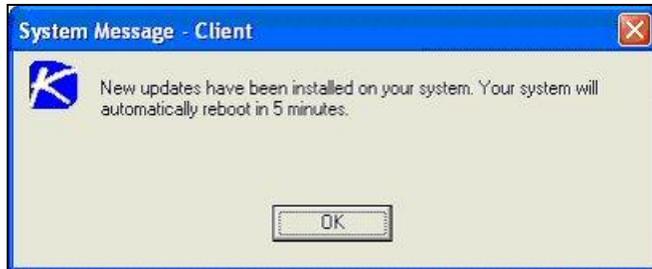
Reboots the computer immediately after the install completes.

## Reboot <day of week> at <time of day> after install.

After the patch install completes, the computer is rebooted at the selected day of week and time of day. Use these settings to install patches during the day when users are logged in, then force a reboot in the middle of the night. Selecting **every day** reboots the machine at the next specified time of day following the patch installation.

**Warn user that machine will reboot in <N> minutes (without asking permission).**

When the patch install completes, the message below pops open warning the user and giving them a specified number of minutes to finish up what they are doing and save their work. If no one is currently logged in, the system reboots immediately.

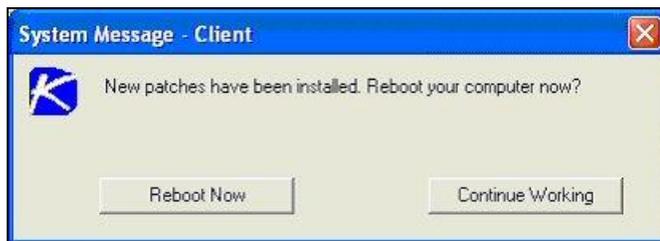


**Skip reboot if user logged in.**

If the user is logged in, the reboot is skipped after the patch install completes. Use this setting to avoid interrupting your users. This is the default setting.

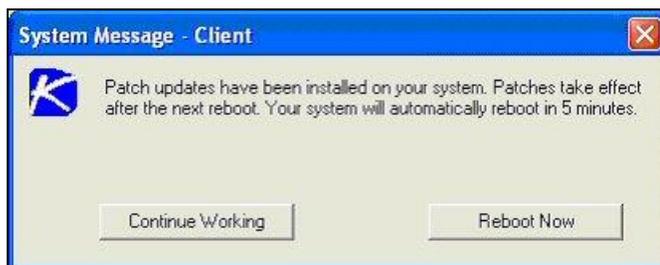
**If user logged in ask to reboot every <N> minutes until the reboot occurs.**

This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears every N minutes repeatedly, until the system has been rebooted. If no one is currently logged in, the system reboots immediately.



**If user logged in ask permission. Reboot if no response in <N> minutes. Reboot if user not logged in.**

This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, it reboots automatically after N minutes **without saving** any open documents. If no one is currently logged in, the system reboots immediately.



**If user logged in ask permission. Do nothing if no response in <N> minutes. Reboot if user not logged in.**

This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, the reboot is skipped. If no one is logged in, reboot immediately.



### **Do not reboot after update**

Does not reboot. Typically used if the machine is a server and you need to control the reboot. You can be notified via email when a new patch has been installed by checking [Email when reboot required](#) and filling in an email address. You can also format the email message by clicking the [Format Email](#) button. This option only displays for [master role users](#) (page 600).

The following types of patch reboot emails can be formatted:

- Patch Reboot

**Note:** Changing the email alarm format changes the format for all [Patch Reboot](#) emails.

The following variables can be included in your formatted email alerts and in procedures.

<b>Within an Email</b>	<b>Description</b>
<at>	alert time
<db-view.column>	Include a <a href="#">view.column</a> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	group ID
<id>	machine ID

### **Run select agent procedure before machine is rebooted**

If checked, the selected agent procedure is run just *before* the machine is rebooted.

### **Run select agent procedure after machine is rebooted**

If checked, the selected agent procedure is run just *after* the machine is rebooted.

### **Select All/Unselect All**

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### **Check-in status**

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

- Online but waiting for first audit to complete

## Patch Management

-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Reboot Action

The type of reboot action assigned to each machine ID.

---

## File Source

### Patch Management > File Source

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [File Source](#) page defines where each machine gets patch executable files from, prior to installation, and where these patch executables are copied to the local machine. File source locations include:

- The internet
- The KServer
- A file share

**Note:** Selecting the File share located on option below affects where Backup and Endpoint Security is installed from.

**Note:** Patch download links with a `.cab` extension are always downloaded directly from the internet regardless of the File Source setting.

### View Definitions

You can filter the display of machine IDs on any agent page using the [Machines with Patch File Source configuration](#) option in [View Definitions](#) (page 28).

### Apply

Click [Apply](#) to apply the selected patch source option to selected machine IDs.

### Copy packages to working directory on local drive with most free space

Patches are downloaded, or copied from a file share, to the managed machine's hard disk. Several patches, especially service packs, may require significant additional local disk space to completely install. Check this box to download patches to the [Working Directory](#) (page 78), but use the drive on the managed machine with the most free disk space. Uncheck this box to always use the drive specified in [Working Directory](#) for the machine ID.

## Delete package after install (from working directory)

The install package is typically deleted after the install to free up disk space. Uncheck this box to leave the package behind for debugging purposes. If the install fails and you need to verify the [Command Line \(page 348\)](#) switches, do not delete the package so you have something to test with. The package is stored in the [Working Directory](#) on the drive specified in the previous option.

## Download from Internet

Each managed machine downloads the patch executable file directly from the internet at the URL specified in [Patch Location \(page 351\)](#).

## Pulled from system server

First the KServer checks to see if it already has a copy of the patch file. If not, the new patch executable is downloaded automatically and stored on the KServer, then used for all subsequent distributions to managed machines. When a patch needs to be installed on a managed machine, this patch file is pushed to that machine from the KServer.

**Note:** The location for patch files stored on the KServer is <Kaseya installation directory>\WebPages\ManagedFiles\VSAPatchFiles\

## Clear Cache

Click [Clear Cache](#) to clear all downloaded patches stored on the KServer.

## Pulled from file server using UNC path

This method is recommended if you support many machines on the same LAN.

Patch files are downloaded to the local directory of a selected machine ID. The local directory on the machine ID is configured to be shared with other machine IDs on the same LAN. All other machine IDs on the same LAN use a UNC path to the shared folder located on the first machine ID. All other machines on the same LAN require a credential to access the shared folder on the first machine and install the patch files. A credential is specified for the first machine with the shared directory using Agent > [Set Credential \(page 83\)](#).

### Setup

1. Enter a UNC path in the [Pulled from file server using UNC path](#) field. For example, \\computername\sharedname\dir\.
2. Use the [Machine Group Filter](#) drop-down list to select a group ID.
3. Select a machine ID from the [File share located on](#) drop-down list.
4. Enter a shared local directory in the [in local directory](#) field.

**Note:** The value in the [in local directory](#) field must be in full path format, such as c:\sharedir\dir.

- First the KServer checks to see if the patch file is already in the file share. If not, the machine ID with the file share automatically loads the patch file either directly from the internet or gets it from the KServer. In either case, the managed machine with the file share **must have an agent** on it.
  5. [File Server automatically gets patch files from](#) - Select one of the following options:
    - [the Internet](#) - Use this setting when the managed machine running the file share has full internet access.
    - [the system server](#) - Use this setting when the managed machine running the file share is blocked from getting internet access.
  6. [Download from Internet if machine is unable to connect to the file server](#) - Optionally check this box

## Patch Management

to download from the internet. This is especially useful for laptops that are disconnected from the company network but have internet access.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Patch Source

Lists the patch source selected for each machine ID. A [Clear Cache](#) button displays in this column if the [Pulled from file server using UNC path](#) option is selected for a machine ID. Clicking this [Clear Cache](#) button clears patches from the specified file server UNC path. The [Clear Cache](#) button is *not* machine specific. All patches stored on that file server for the specified path will be deleted.

---

## Patch Alert

### Patch Management > Patch Alert

#### Monitor > Alerts (page 219)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench
- Select Patch Alert from the [Select Alert Function](#) drop-down list.

The [Alerts - Patch Alert](#) (page 249) page triggers an alert for patch management events on managed machines.

- A new patch is available for the selected machine ID.
- A patch installation failed on the selected machine ID.
- The agent credential is invalid or missing for the selected machine ID.
- Windows Auto Update changed.

## To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
  - Create **A**larm
  - Create **T**icket
  - Run **S**cript
  - **E**mail Recipients
2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the **A**pply button.

## To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the **C**lear button.  
The alert information listed next to the machine ID is removed.

## Passing Alert Information to Emails and Procedures

The following types of patch alert emails can be sent and formatted:

- New Patch Available
- Patch Install Failed
- Patch Approval Policies Updated
- Agent Credential Invalid
- Windows Auto Update Configuration Changed

**Note:** Changing the email alarm format changes the format for all **Patch Alert** emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<au>	#au#	auto update change
<bi>	#bi#	bulletin ID
<bl>	#bl#	new bulletin list
<db-view.column>	not available	Include a <b>view.column</b> (page 477) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<fi>	#fi#	failed bulletin ID
<gr>	#gr#	group ID
<ic>	#ic#	invalid credential type
<id>	#id#	machine ID
<pl>	#pl#	new patch list
	#subject#	subject text of the email message, if an email was sent in response to an alert

## Patch Management

	#body#	body text of the email message, if an email was sent in response to an alert
--	--------	--

### Create Alarm

If checked and an **alarm condition** (*page 585*) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (*page 189*), Monitor > **Alarm Summary** (*page 198*) and Info Center > Reports > Logs > Alarm Log.

### Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

### Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (*page 94*) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

### Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (*page 391*).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for **master role users** (*page 600*).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (*page 426*).

### Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

### Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

### Patch Alert Parameters

The system can trigger an alert for the following alarm conditions for a selected machine ID:

- **New patch is available**
- **Patch install fails**
- **Agent credential is invalid or missing**

**Note:** An agent credential (page 588) is not required to install patches unless the machine's File Source (page 340) is configured as Pulled from file server using UNC path. If an agent credential is assigned, it will be validated as a local machine credential without regard to the File Source configuration. If this validation fails, the alert will be raised. If the machine's File Source is configured as Pulled from file server using UNC path, a credential is required. If it is missing, the alert will be raised. If it is not missing, it will be validated as a local machine credential and as a network credential. If either of these validations fails, the alert will be raised.

- **Windows Auto Update changed**

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Approval Policy Updated

Displays as the first row of data. If selected and the **Apply** button clicked, an alert is generated when a new patch is added to all patch policies. See **Patch Approval Policy** (page 595). This is a system alert and not associated with any machines.

### ATSE

The ATSE response code assigned to machine IDs:

- A = Create **A**larm
- T = Create **T**icket
- S = Run Procedure
- E = **E**mail Recipients

## Patch Management

### Email Address

A comma separated list of email addresses where notifications are sent.

### New Patch

If checked, an alarm is triggered when a new patch is available for this machine ID.

### Install Failed

If checked, an alarm is triggered when a patch installation has failed for this machine ID.

### Invalid Credential

If checked, an alarm is triggered when the credential is invalid for this machine ID.

### Win AU Changed

If checked, an alarm is triggered if the group policy for **Windows Automatic Update** on the managed machine is changed from the setting specified by Patch Management > **Windows Auto Update** (page 335).

**Note:** A log entry in the machine's Configuration Changes log is made regardless of this alert setting.

---

## Office Source

### Patch Management > Office Source

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Office Source** page sets *alternate* source locations for installing Office and Office component applications. The source location can be changed from the default CD-ROM, which is the typical installation source, to a network share or a directory on a local hard drive. By changing the installation source to a network share or a local directory, those patches that require the Office installation source for installation can get access **without prompting the user for the installation media**. This alternate source location can be configured to be read-only. It must contain an exact copy of the installation media contents including all hidden files and/or directories.

An Office source for a managed machine is only available after you have run **Scan Machine** (page 310) at least once for the managed machine. Machine IDs are displayed on this page only if they:

- Currently match the **Machine ID / Group ID filter** (page 26).
- Have Office or Office component applications installed for Office 2000, XP, or 2003.

**Note:** Office 2007 is not displayed on this page. Office 2007 installs a full set of source installation files on a machine, so an alternate source location is not required.

### Multiple Entries

Multiple entries may be displayed for a machine because the machine contains one or more Office component applications, such as FrontPage or Project, that were installed separately from their own installation source and were not part of the Office installation.

### Credential Required

Managed machines must have a **credential set** (page 83) to use the Office Source page. The agent must have a credential to use the alternate Office source location.

### Validation

The specified location is validated to be sure that the location is accessible from the machine and that the installation source in the specified location contains the correct edition and version of Office or the

Office component application. Only after the validation succeeds is the machine's registry modified to use the specified location.

## Installing Office Products

Some patches—particularly Office service packs—still display progress dialogs even though the silent installation switch (/Q) is included using Patch Management > [Command Line](#) (page 348). These progress dialogs do not require any user intervention.

Some patches and service packs display a modal dialog indicating the update has completed, again even though the silent installation switch (/Q) is used. This requires the user to click on the OK button to dismiss the dialog. Until this happens, the patch installation procedure appears to be hung and will not complete until this dialog is dismissed!

Some Office service packs fail for no apparent reason. Checking the machine's application event log reveals that another Office component service pack failed. This has been observed with Office 2003 service pack 2 requiring the availability of FrontPage 2003 service pack 2. When the Office source location for the FrontPage 2003 is configured, the Office 2003 service pack 2 finally successfully installs.

## Filter on Office Product

Because each managed machine may be listed multiple times—once for each Office product or Office component application installed—you can filter the Office products/components displayed. This ensures selecting the same product code for multiple machines when setting the installation source location.

## Apply

Click [Apply](#) to apply the Office source location specified in [Location of Office installation source](#) to selected machine IDs.

## Location of Office installation source

Add the network share as a UNC path (i.e., \\machinename\sharename) or a local directory as a fully qualified path (i.e., C:\OfficeCD\Office2003Pro) in the installation source text box.

## Reset

Click [Reset](#) to restore selected machine IDs back to their original installation source, typically the CD-ROM.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Status

Displays one of the following:

- Missing Credential
- Update Procedure Failed
- Validation Procedure Failed
- Original Source
- Pending Validation
- Updating Machine
- Incorrect Edition
- Processing Error
- Restoring Original
- Office Source Updated

### Office Product

Displays the name of the Office product.

### Office Source

Displays the current installation source location for this Office product on this machine ID.

### Product Code

Displays the Office product code.

---

## Command Line

### Patch Management > Command Line

- This page applies to the following product: On Premises

The **Command Line** page defines the command line switches used to silently install a specified patch. Occasionally a patch is released that does not use normal switch settings or the patch database has not been updated with the new switches. If you find a patch does not successfully install with its assigned switch settings, you can change them with this page. Locate patch switches by clicking the **KB Article** link and reading through the knowledge base article.

**Warning:** Changes to the switches effect all users. This page only displays for master role users (page 600).

### Suppress Automatic Reboot

Usually you want to load a patch without requiring any user interaction at all. The system supports batch installs of multiple patches at the same time and reboots once at the end of all patch installations. Therefore, use switch settings to suppress automatic reboot wherever possible.

### Switch Settings

Typical patch file switch settings for **silent, unattended installs without reboot**:

- `/quiet /norestart` - This is the standard setting for most patches in recent years.

- /u /q /z - Typical switch settings used to silently install older patches that do not use the Windows Installer technology.
- /m /q /z - Typical switch settings to silently install older patches released for Windows NT4.
- /q:a /r:n - Internet Explorer and other application switch settings to install in quiet user mode (/q:a) and not automatically reset (/r:n) when the install completes.
- Other switch settings found with Microsoft patch installations include:
  - /? - Display the list of installation switches.
  - /u - Use Unattended mode.
  - /m - Unattended mode in older patches.
  - /f - Force other programs to quit when the computer shuts down.
  - /n - Do not back up files for removal.
  - /o - Overwrite OEM files without prompting.
  - /z - Do not restart when the installation is complete.
  - /q - Use quiet mode (no user interaction).
  - /l - List the installed hotfixes.
  - /x - Extract files without running Setup.

### Microsoft Office command line switches

The only switch permitted for use with Microsoft Office 2000 and Office XP related patches is /Q. If /Q is not specified, Microsoft Office 2000 and Microsoft Office XP switches will be automatically reset to /INSTALL-AS-USER. Microsoft Office 2003 patches may also include the /MSOCACHE switch used to attempt a silent install if the MSOCache exists on the machine. These settings are enforced by the application.

**Note:** The /MSOCACHE switch only applies to Office 2003. When the patch database is updated, this switch is automatically added to all Office 2003 patches where a user has never modified a particular patch's command line switches. It is not automatically added to Office 2003 service packs. When this switch is used, the system determines if the MSOCache exists on the target machine. If the MSOCache does exist and this switch is used, the system automatically uses the run silently switch (/Q) thereby relying on the MSOCache rather than requiring the actual installation media. If the MSOCache does not exist on the target machine, the existing switch is used. If a patch installation fails that uses the /MSOCACHE switch, it typically means that the MSOCache could not be used by the patch. In this case, you must clear out all command line switches for this patch and set the /INSTALL-AS-USER switch. Re-running the patch installation should now succeed. Unfortunately, this requires user intervention and also probably requires the Office 2003 installation media.

### Server-side command line switches

Special server-side command line switches can be combined with patch specific switches:

- /INSTALL-AS-USER - Tells the system to only install this patch as a user. Some rare patches do not install successfully unless someone is logged onto the machine. Add this switch if you find a patch is failing to install if no one is logged in.

**Warning:** This setting conflicts with the Skip update if user logged in setting found in Reboot Action (page 337). /INSTALL-AS-USER requires that a user be logged in to install.

- /DELAY-AFTER=xxx - After the install wait xxx seconds before performing the reboot step. The reboot step starts after the install package completes. Some rare installers spawn additional programs that must also complete before rebooting. Add this switch to give other processes time to complete after the main installer is done.

## Patch Management

### Patch Data Filter Bar

You can filter the data displayed by specifying values in each field of the [Patch Data Filter Bar](#) at the top of the page.



The screenshot shows a horizontal filter bar with three input fields: 'KB Article: \*', 'Classification: \*', and 'Product: \*'. To the right of these fields is a magnifying glass icon followed by the text 'Apply'. Further right is a dropdown menu labeled 'Patch View: kadmin Patch View' with a downward arrow. To the right of the dropdown are two icons: a pencil icon labeled 'Edit' and a trash can icon labeled 'Reset'.

Enter or select values in the [KB Article](#), [Classification](#) or [Products](#) fields. You can also click the [Edit...](#) button to filter by additional fields and save the filtering selections you make as a view. Supports [advanced filtering](#) (*page 30*) logic. Saved views can be shared using the [Make Public \(others can view\)](#) checkbox when editing the view.

### Filter patches by

Based on the patch category selected, this page displays all patches and service packs for all machines, both missing and installed, that match the current [Machine ID/Group ID filter](#) (*page 592*).

### New Switches

Enter the command line switches you want to apply to selected patches.

### Apply

Click [Apply](#) to apply the specified command line switches to selected patches.

### Reset

Click [Reset](#) to reset the command lines of selected patches back to their default settings.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

### Patch Name

The patch install filename.

### Security Bulletin

Click the [Security Bulletin](#) link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSYY-xxx).

### Product

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

### Office?

If an Office product, the version displays.

### Switches

The command line switches used to install this patch.

---

# Patch Location

## Patch Management > Patch Location

- This page applies to the following product: On Premises

The **Patch Location** page defines the URL from which each patch is downloaded. Only patches *missing* from machine IDs that currently match the **Machine ID / Group ID filter** (page 26) are displayed here. You should consult this page if, when attempting to install a patch, you are notified of a `Path Missing`.

The KServer maintains a list of each patch and the URL it should be downloaded from. In most cases the download URLs provided for patches are correct. `Path Missing` errors may occur for the following reasons:

- Each language may require a separate URL to download from.
- The URL may change for one or more patches.
- The KServer's record for the URL may be entered incorrectly or be corrupted.

In such cases, users can change the download path associated with a patch. Manually entered URLs are shown in **dark red**.

**Note:** Changes effect patches installed by all users. This page only displays for master role users (page 600).

### To find the URL to a missing path

1. Click the **KB Article** listed for the missing path.
2. Read through the knowledge base article and locate the download URL for the patch.

**Note:** There may be several products referenced by the same **KB Article**. For instance, each Windows operating system is a different product. Also, patches can be different for specific service packs of the operating system.

3. Click on the download link for your patch. If a *different patch is available for each language*, you will be prompted to select a language.
4. Select the appropriate language for the download, if applicable.
5. Click the **Download** link or button and download the patch file.
6. On your web browser, click the **History** icon to view your URL history.
7. Locate the file you just downloaded from your history list. Typically, the file will be in the `download.microsoft.com` domain.
8. Right-click the filename you just downloaded and select **Copy** from the menu. This copies the entire URL into your clipboard.
9. Return to the **Patch Location** page and:
  - a. Paste the URL into the **New Location** edit box.
  - b. Select the radio button to the left of the **KB Article** for which you are entering a new patch location.
  - c. Click the **Apply** button.

### Patch Data Filter Bar

You can filter the data displayed by specifying values in each field of the **Patch Data Filter Bar** at the top of the page.

The screenshot shows a horizontal filter bar with the following elements from left to right: a text input field for 'KB Article', a dropdown menu for 'Classification', a text input field for 'Product', a magnifying glass icon followed by the text 'Apply', a dropdown menu for 'Patch View' currently showing 'kadmin Patch View', a pencil icon followed by the text 'Edit', and a trash can icon followed by the text 'Reset'.

Enter or select values in the **KB Article**, **Classification** or **Products** fields. You can also click the **Edit...** button to filter by additional fields and save the filtering selections you make as a view. Supports **advanced filtering** (page 30) logic. Saved views can be shared using the **Make Public (others can view)** checkbox when editing the view.

## Patch Management

### New Location

Enter a new URL.

### Apply

Click [Apply](#) to apply the URL listed in the [New Location](#) field to the selected patch.

### Remove

Click [Remove](#) to delete the download URL associated with a patch ID.

**Warning:** Removing a path disables patching managed machines using this patch until the correct path is entered.

### KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

### Security Bulletin

Click the [Security Bulletin](#) link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSYY-xxx).

### Product

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

### Language

The language associated with the patch location.

## Chapter 9

# Remote Control

### In This Chapter

Remote Control Overview	355
Control Machine	356
Video Streaming	359
Reset Password	360
Select Type	362
Set Parameters	363
Preinstall RC	364
Uninstall RC	366
User Role Policy	367
Machine Policy	368
FTP	370
Task Manager	372
Chat	373
Send Message	375
Power Management	377
Remote ISO Boot	378
Live Connect	380

## **Remote Control**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# Remote Control Overview

View and operate managed machines as if they were right in front of you simply by clicking its machine ID. The **Remote Control** module enables you to:

- Automatically connect the user to the remote computer independent of any gateway or firewall configurations, even behind NAT.
- Remote control even without an agent using video streaming.
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time.
- Set policies that allow users to block remote control or require users to ask permission before accessing a machine.
- Use four best of breed remote control packages: WinVNC, pcAnywhere™ (Symantec), RAdmin (Famatech), or Terminal Server (Microsoft).
- FTP to any managed machine and access files even behind NAT gateways and firewalls.
- Direct chat with any managed machine. Perfect for supporting dial up users with only a single phone line. Remote control and chat at the same time.
- Power up, power down, bootup or reboot vPro-enabled machines.
- Use **Live Connect** to perform tasks and functions solely for one managed machine. *Click any check-in icon next to any machine ID in the VSA.*

---

Functions	Description
<a href="#">Control Machine</a> (page 356)	Allows users to view and/or take control of a managed machine's desktop remotely for troubleshooting and/or instructional purposes.
<a href="#">Video Streaming</a> (page 359)	Remote control machines that do not have an agent installed.
<a href="#">Reset Password</a> (page 360)	Reset the password for a local account on a managed machine.
<a href="#">Select Type</a> (page 362)	Specify the type of remote control software the VSA uses on a per machine basis. WinVNC, Remote User, pcAnywhere, and Terminal Server are all supported.
<a href="#">Set Parameters</a> (page 363)	Specify the remote control settings to use with each remote control package.
<a href="#">Preinstall RC</a> (page 364)	Install the remote control service
<a href="#">Uninstall RC</a> (page 366)	Uninstall the remote control service
<a href="#">User Role Policy</a> (page 367)	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by VSA user role.
<a href="#">Machine Policy</a> (page 368)	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by machine ID.
<a href="#">FTP</a> (page 370)	Initiate an FTP session with any remote managed machine.
<a href="#">Task Manager</a> (page 372)	Remotely executes the NT task manager and displays data in the browser.
<a href="#">Chat</a> (page 373)	Start a chat session between a user and any remote machine.
<a href="#">Send Message</a> (page 375)	Allows users to send network messages to selected managed machines.

---

## Remote Control

<a href="#">Power Management</a> (page 377)	Powers on, powers off or reboots vPro-enabled machines.
<a href="#">Remote ISO Boot</a> (page 378)	Boots VPro machines from an ISO image.
<a href="#">Live Connect</a> (page 380)	Perform tasks and functions solely for one managed machine. <i>Click any check-in icon next to any machine ID in the VSA.</i>

# Control Machine

## Remote Control > Control Machine

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Control Machine](#) page establishes a remote control session between the user's local machine and a selected machine ID.

- Select the type of package to use to remote control a managed machine using [Select Type](#) (page 362).
- Set parameters for remote control sessions using [Set Parameters](#) (page 363).
- Use [Video Streaming](#) (page 359) to remote control a target machine that does not have an agent.

**Note:** You can also use [Live Connect](#) (page 380) to initiate a remote control session with a managed machine.

## Automatic Installation

If [WinVNC](#), [K-VNC](#) or [RAdmin](#) are *not* installed on a machine and a remote control session is initiated using [Control Machine](#) (page 356) or [Video Streaming](#) (page 359), then these packages are automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute. To eliminate this delay during first time use, you can pre-install [WinVNC](#), [K-VNC](#) or [RAdmin](#) on any managed machine using [Preinstall RC](#) (page 364).

**Note:** Uninstalling an agent does not remove the installed Remote Control package, KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > [Uninstall RC](#) (page 366) to uninstall remote control on the managed machine. Uninstall all add-on module clients as well.

## Initiating Remote Control

Initiate remote control by clicking the name of the target machine. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an  or  or  icon can be connected to target machines and have live links; all others will be inactive.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

**Note:** Users can disable remote control and FTP sessions by right-clicking the  icon on their managed machine and selecting **Disable Remote Control**. You can deny users this ability by removing **Disable Remote Control** using [Agent > Agent Menu](#) (page 73).

## ActiveX Control

An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package on a new machine, your browser may ask if it is OK to download and install this ActiveX control. Click yes when asked. If the ActiveX control is blocked by the browser from running, the user is presented with a link to manually download and run the remote control package manually.

## Helper Applications

In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the user machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the VSAuser machine and the remote machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

## Enable verbose relay

Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

## Remote Controlling the KServer

Clicking the [KServer](#) link starts a remote control session to the KServer itself. Use this feature to remotely manage your own KServer. Only master role users can remote control the KServer.

## Remote Control and FTP for Users

VSA users can provide machine users with the same remote control and FTP access using [Agent > Portal Access](#) (page 81).

## Remote Control Malfunctions

Some reasons for remote control failure—for target machines with and without an agent—are:

- The remote machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The remote machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Anti-virus software on the remote machine may block the connection. This problem is eliminated if Endpoint Security protection is installed on the remote machine.
- Wrong primary KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using [Agent > Check-in Control](#) (page 75).
- XP supports only one [RDP/Terminal Service](#) session on the target machine and logs off other users. Starting a remote logon session from a second machine logs off the first remote logon session. The VSA uses the port relay to get through firewalls and gateways. To Windows XP, it appears as if the Terminal Server session is connecting from the localhost.

**Warning:** Using the credential of a currently logged on user confuses XP. It can not determine if the user is reactivating the existing session locally or remotely initiating a new connection. As a result Windows XP may hang, requiring a reboot to recover. The VSA can not protect you from this. Do not log on using the user name of an already logged on account.

## Remote Control

- Your **pcAnywhere** viewer is connecting to your local machine, not the remote machine. The KServer relay is telling the viewer to connect to `localhost`. **If you have a pcAnywhere host running on the machine you are viewing from**, then the viewer connects to it and not the VSA relay. Right click the pcAnywhere icon in the system tray and select **Cancel Host**.
- **pcAnywhere** presents an error dialog saying `Cannot find callhost file: C:\Document and Settings\All Users\Application Data\Symantec\pcAnywhere\Network.CHF`. There is no `Network` remote control item configured in pcAnywhere.
  1. Open the **pcAnywhere** application and click on the **Remote Control** function.
  2. Click **Add Remote Control Item**.
  3. Create an item named **Network**.
  4. Select **TCP/IP** as the connection device.
  5. Leave the host name blank.
  6. Close **pcAnywhere**.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using **Select Type** (page 362).

-  WinVNC
-  K-VNC
-  Remote User
-  pcAnywhere
-  RDP/Terminal Server
-  Apple

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using `System > User Security > Scopes` (page 404). Only machine IDs with an  or  or  icon can be connected to target machines and have live links; all others will be inactive.

## Current User

The user currently logged on to the managed machine.

## Active Admin

The VSA user currently conducting a remote control session to this machine ID.

---

# Video Streaming

## Remote Control > Video Streaming

- This page applies to the following product: On Premises

The **Video Streaming** page establishes a remote control session between the VSA user's local machine and a machine **without an agent**. Use it to help someone quickly on an infrequent basis. If you plan to provide continuous support we recommend you install an agent.

The following conditions apply:

- The remote user must log into a URL after the user has started the video streaming session.
- The remote user must have user privileges on the local machine.
- Each VSA user can only initiate a single video streaming session at a time.

Set parameters for remote control sessions using **Set Parameters** (page 363). See **Select Type** (page 362) for a description of the different types of remote control packages.

**Note:** Use **Control Machine** (page 356) to remote control a target machine that has an agent.

## Automatic Installation

If **WinVNC**, **K-VNC** or **RAdmin** are *not* installed on a machine and a remote control session is initiated using **Control Machine** (page 356) or **Video Streaming** (page 359), then these packages are automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute.

## Automatic Uninstallation

When either side terminates the **Video Streaming** session, the remote server on the target machine uninstalls automatically, removing all remote control files and registry additions.

## ActiveX Control

An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package on a new machine, your browser may ask if it is OK to download and install this ActiveX control. Click yes when asked. If the ActiveX control is blocked by the browser from running, the user is presented with a link to manually download and run the remote control package manually.

## Helper Applications

In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the user machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the VSAuser machine and the remote machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

## Remote Control Malfunctions

Some reasons for remote control failure—for target machines with and without an agent—are:

- The remote machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The remote machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.

## Remote Control

- Anti-virus software on the remote machine may block the connection. This problem is eliminated if Endpoint Security protection is installed on the remote machine.
- Wrong primary KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using Agent > [Check-in Control](#) (page 75).

## Start

Click the [Start](#) button. Ask the remote user to display the `http://<yourKServerURL>/gethelp.asp` web page and click your user name to begin the video streaming session.

## Enable verbose relay

Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

## Select remote control package to use

The default remote control service uses [WinVNC](#). See [Select Type](#) (page 362) for a description of the different types of remote control packages.

-  WinVNC
-  K-VNC
-  Remote User

## Specify the default HTML message seen by users when no administrator is waiting to help.

This is the message displayed if the remote user displays the `http://<yourKServerURL>/gethelp.asp` web page and no VSA user is logged into the KServer. After making changes to this message, click the [Apply](#) button to save it. Click [Default](#) to reset the message back to its default setting.

---

# Reset Password

## Remote Control > Reset Password

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Reset Password](#) page creates a new password and, if necessary, a new user account on a managed machine. It can also change domain user accounts on domain name controllers.

If the username does not already exist, checking the [Create new account](#) checkbox creates a new account with the specified password. [Reset Password](#) returns an error if you attempt to reset the password for a username that is not already created on the managed machine or if you create a password that is already being used by a user account. Blank passwords are not permitted.

**Note:** To delete a user account, you can create a procedure to delete the user account or use remote control to manually delete the user account.

## Resetting the User Password

Use [Reset Password](#) to reset the user password on all your managed machines when:

- Your user password is compromised.

- Someone leaves your organization who knew the user password.
- It is time to change the user password as part of a good security policy.

**Note:** On non-domain controllers, only the local user account on the remote machine is changed. On domain controllers, **Reset Password** changes the domain user accounts.

### Apply

Click **Apply** to apply password and user account parameters to selected machine IDs.

### Cancel

Click **Cancel** to clear pending password changes and user account creations on selected machine IDs.

### Username

Enter the username on the managed machine.

### Create new account

Check this box to create a new user account on the managed machine.

### as Administrator

Check this box to create the new user account with administrator privileges.

### Password / Confirm

Enter a new password.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Status

The status of pending password changes and user account creations.

## Select Type

### Remote Control > Select Type

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Select Type** page specifies which remote control package is used by **Control Machine** (page 356) to remote control a managed machine. You can assign different packages to different machines. Each machine ID displays the icon of the remote control package it is currently assigned to use.

### Virtual Network Computing

**Virtual Network Computing (VNC)**, also called **remote control** or **remote desktop**, is a graphical desktop sharing system which uses the Remote Framebuffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. It is included with the KServer primarily to provide immediate technical support. VNC is platform-independent. A VNC viewer on any operating system can usually connect to a VNC server on any other operating system. The **VNC server** is the program on the remote machine that shares its screen. The **VNC client (or viewer)** is the program on the local machine that watches and interacts with the remote machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the KServer, all VNC sessions are protected by the Kaseya 256 bit rolling encryption protocol.

### Select remote control package to use with selected machines

The VSA supports the following third party remote control packages.

- **WinVNC**  - This open source, freely available, remote control package comes bundled with the VSA. WinVNC is the default package used to remote access all managed machines.

**Note:** For Linux agents, the VSA automatically installs x11vnc servers on selected machines the first time you remote control that machine. Use either WinVNC to K-VNC to remote access Linux machines.

- **K-VNC**  - The enterprise version of VNC. *This is the only remote control option available for Vista, Windows 7, and Windows Server 2008.* It can also be used on Windows 2000, XP, 2003, and Macintosh OS X 10.4.x (Tiger) and 10.3.x (Panther). The VSA automatically installs the K-VNC server on selected machines the first time you remote control that machine.
- **Remote User**  - RAdmin is a commercially available remote control package offering both high speed and file transfer capability. Use RAdmin where bandwidth limitations exist or you need remote file transfer to the machine. The VSA automatically installs the RAdmin server on selected machines the first time you remote control that machine. The RAdmin package bundled with the VSA expires after 30 days. Obtain licenses from [www.radmin.com](http://www.radmin.com) (<http://www.radmin.com>).
- **pcAnywhere**  - pcAnywhere is a widely used remote control package available from Symantec. The VSA fully supports pcAnywhere but does not automatically install it. You must purchase pcAnywhere separately and install it on the workstation before you can use this option. Combining the VSA with existing installations of pcAnywhere allows you to remote control machines behind gateways without mapping ports or opening firewalls.
- **Terminal Server**  - Microsoft Terminal Server is only available with Windows NT, 2000, XP, Vista, Windows 7, 2003 or 2008. The VSA does not automatically install Terminal Server but does allow you to remote control machines behind gateways without mapping ports or opening firewalls. XP, Vista and Windows 7 come pre-installed with Terminal Service access for a single user. For other operating systems see **Terminal Service Client Access License requirements** (<http://technet2.microsoft.com/windowsserver/en/technologies/featured/termserv/tslicensing.mspx>) on the Microsoft website.

- **Apple VNC Server & UltraVNC viewer combination**  - UltraVNC is an open source, freely available, remote control viewer which comes bundled with the VSA. The Apple VNC Server is built-in into Mac OS X 10.5 and above. The combination of the UltraVNC viewer with Apple's built-in VNC Server is used on all managed machines running Mac OS X 10.5 and above. This is the only remote control option available for Mac OS X 10.5 (Leopard) and above (including Snow Leopard). The VSA automatically installs the UltraVNC viewer on the admin side the first time you remote control any of the supported Mac systems.

### To Assign Remote Control Packages to Machine IDs

1. Select the type of package to use from the drop-down list.
2. Check the box to the left of machine IDs you want to use this remote control package.
3. Click the **Select** button.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

### Remote Control Package

The remote control package assigned to this machine ID.

-  WinVNC
-  K-VNC
-  Remote User
-  pcAnywhere
-  RDP/Terminal Server

---

## Set Parameters

### Remote Control > Set Parameters

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

## Remote Control

The **Set Parameters** page sets the default parameters for your remote control session. *These settings are remembered on a per VSA user basis. Changes take effect immediately and are reused every time you start remote control.* See **Select Type** (page 362) for a description of the different types of remote control packages.

### WinVNC and K-VNC Options

- **View Only Mode** - You can view the remote machine. No mouse or keyboard events are sent to the remote machine.
- **Hide WinVNC system tray icon on the remote machine** - Check this box to hide the WinVNC icon on the remote machine.
- **Restrict to 64 colors** - The display is set to 64 colors. This is useful for slower connections.
- **Full Screen mode** - The entire display of your local machine is used to display the screen contents of the remote machine. Exit by displaying the remote control menu (default **F8**) and unselect **Full screen**.

### RAdmin Options

- **Full Control** - You can view and/or control the screen keyboard and mouse of the remote machine.
- **View Only** - You can view the remote machine. No mouse or keyboard events are sent to the remote machine.
- **File Transfer** - Start a file transfer (FTP) session with the remote machine. This mode presents you with two standard file browsers, one for the remote machine and one for your local machine. Drag and drop files between the two machines in this mode.
- **Full Screen View Mode** - The entire display of your local machine is used to display the screen contents of the remote machine. This option is only available for Full Control or View Only sessions.
- **Encrypt Data Stream** - Checking this box encrypts all traffic between your local machine and the remote machine.
- **Updates/sec** - Sets the maximum number of updates per second RAdmin generates. Higher update rates consume more CPU cycles on the remote machine.
- **Color Format** - Specifies the number of colors used for remote control. Large color formats use more bandwidth.

### Terminal Service Options

- **Console mode** - Remote control the console session of the remote machine.
- **Full Screen mode** - Use your full screen to remote control the remote machine.
- **Fixed Screen size** - Set a fixed width and height for your remote control session.
- **Share Disk Drives** - Connect your disk drives to the remote machine.
  - **Only share the following disks** - Enter the specific drive letters to share, or leave blank to share all disks.
- **Share Printers** - Connect your printers to the remote machine.
- **Disable Desktop Wallpaper** - Turn off wallpaper on the remote machine for faster processing.

---

## Preinstall RC

### Remote Control > Preinstall RC

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Preinstall RC** page installs **WinVNC**, **K-VNC** or **RAdmin** on selected machine IDs without initiating a remote control session. Select the type of package to remote control a managed machine using **Select Type** (page 362). When an install is pending on any machine ID this page automatically refreshes every 5

seconds until the procedure completes.

**Note:** Preinstall RC does not install [pcAnywhere](#) or [Terminal Server](#).

## Automatic Installation

If [WinVNC](#), [K-VNC](#) or [RAdmin](#) are *not* installed on a machine and a remote control session is initiated using [Control Machine](#) (page 356) or [Video Streaming](#) (page 359), then these packages are automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute. To eliminate this delay during first time use, you can pre-install [WinVNC](#), [K-VNC](#) or [RAdmin](#) on any managed machine using [Preinstall RC](#) (page 364).

**Note:** Uninstalling an agent does not remove the installed Remote Control package, KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > [Uninstall RC](#) (page 366) to uninstall remote control on the managed machine. Uninstall all add-on module clients as well.

## Install

Click [Install](#) to install [WinVNC](#), [K-VNC](#) or [RAdmin](#) on selected machine IDs.

## Cancel

Click [Cancel](#) to clear pending install procedures for selected machine IDs.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using [Select Type](#) (page 362).

-  WinVNC
-  K-VNC
-  Remote User
-  pcAnywhere

## Remote Control



RDP/Terminal Server



Apple

## Last Status

*Pending* indicates the install will run the next time that machine checks into the KServer. Otherwise, this column displays when the remote control package was installed on the machine ID.

---

# Uninstall RC

## Remote Control > Uninstall RC

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Uninstall RC** page uninstalls **WinVNC**, **K-VNC** or **RAdmin** on selected machine IDs. Multiple types of remote control packages may be installed on a single machine ID. Select the type of package to uninstall from a managed machine using **Select Type** (page 362). When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the procedure completes.

If an existing installation of **WinVNC** or **RAdmin** has problems then the VSA may not be able to establish a remote control session. If remote control fails then running **Uninstall RC** on that machine ID cleans out any existing problem installs. A fresh copy of the remote control package is installed the next time a remote control session is started or using **Preinstall RC** (page 364).

**Note:** **Uninstall RC** does not uninstall **pcAnywhere** or **Terminal Server**.

**Note:** Uninstalling an agent does not remove the installed Remote Control package, KBU client, KES client, or KDPM client. Before you delete the agent, use **Remote Control > Uninstall RC** (page 366) to uninstall remote control on the managed machine. Uninstall all add-on module clients as well.

## Automatic Uninstallation

**Uninstall RC** is not required for **Video Streaming**. When either side terminates the **Video Streaming** session, the remote server on the target machine uninstalls automatically, removing all remote control files and registry additions.

## Uninstall

Click **Uninstall** to uninstall **WinVNC**, **K-VNC** or **RAdmin** on selected machine IDs.

## Cancel

Click **Cancel** to clear pending uninstall procedures for selected machine IDs.

## Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).



Online but waiting for first audit to complete



Agent online



Agent online and user currently logged on.



Agent online and user currently logged on, but user not active for 10 minutes

-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using [Select Type](#) (page 362).

-  WinVNC
-  K-VNC
-  Remote User
-  pcAnywhere
-  RDP/Terminal Server
-  Apple

## Last Status

*Pending* indicates the uninstall will run the next time that machine checks into the VSA. Otherwise, this column displays when the remote control package was uninstalled on the machine ID.

---

# User Role Policy

## Remote Control > User Role Policy

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **User Role Policy** page determines how you want to notify users that a remote control session to their machine is about to begin. Policies are applied by **user roles** (page 400).

**Note:** See [Machine Policy](#) (page 368) to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

## Apply

Click **Apply** to apply policy parameters to selected machine IDs.

## Select User Notification Type

- **Silently take control** - Do not tell the user anything. Take control immediately and silently.
- **If user logged in display alert** - Display notification alert text. The alert text can be edited in the text box below this option.
- **If user logged in ask permission** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.
- **Require Permission. Denied if no one logged in** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. The remote control session is cancelled.

## Remote Control

### Notify user when session terminates.

Check this box to notify the user when the session terminates.

### Session Termination Message

Displays only if the **Notify user when session terminates** box is checked. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

### Notification Alert Text / Ask Permission Text

Displays only if the **Select User Notification Type** is *not* `Silently take control`. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

### Remove

Click **Remove** to clear policy parameters from selected machine IDs.

### Require admin note to start remote control

Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Delete

Click the delete icon  next to a user role to clear the policy.

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### Role Name

The list of **user roles** (*page 400*).

### Policy

The remote control policy applied to a user role.

### Message

The text messages applied to a user role.

---

## Machine Policy

### Remote Control > Machine Policy

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Machine Policy** page determines how you want to notify users a remote control session to their machine is about to begin. This policy is applied to **machine IDs**.

**Note:** See **User Role Policy** (*page 367*) to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

## Apply

Click [Apply](#) to apply policy parameters to selected machine IDs.

## Select User Notification Type

- [Silently take control](#) - Do not tell the user anything. Take control immediately and silently.
- [If user logged in display alert](#) - Display notification alert text. The alert text can be edited in the text box below this option.
- [If user logged in ask permission](#) - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the [Yes](#) button. If nothing is clicked after one minute, [No](#) is assumed and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.
- [Require Permission. Denied if no one logged in](#) - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the [Yes](#) button. If nothing is clicked after one minute, [No](#) is assumed and the VSA removes the dialog box from the target machine. The remote control session is cancelled.

## Notify user when session terminates.

Check this box to notify the user when the session terminates.

## Session Termination Message

Displays only if the [Notify user when session terminates](#) box is checked. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

## Notification Alert Text / Ask Permission Text

Displays only if the [Select User Notification Type](#) is *not* [Silently take control](#). Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

## Remove

Click [Remove](#) to clear policy parameters from selected machine IDs.

## Require admin note to start remote control

Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Delete

Click the delete icon  next to a machine ID to clear the policy.

## Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

## Remote Control

### Policy

The remote control policy applied to a machine ID.

### Message

The text messages applied to a machine ID.

---

## FTP

### Remote Control - FTP

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [FTP](#) page establishes an FTP session between the user's local machine and a selected machine ID. Once the FTP session is initiated, a new browser window pops up displaying the contents of a fixed disk on the managed machine. Just drag and drop files as you normally would.

**Note:** You can also use [Live Connect \(page 380\)](#) to initiate an FTP session with a managed machine.

### File Transfer Protocol (FTP)

**File Transfer Protocol (FTP)** is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. The **FTP server** is the program on the target machine that listens on the network for connection requests from other computers. The **FTP client** is the program on the VSA user's local machine that initiates a connection to the server. The FTP client machine requires user access rights to the FTP server machine. It is included with the KServer primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. Since Kaseya FTP sessions are relayed through the KServer, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

### Initiating FTP

Initiate an FTP session by clicking the name of the remote machine. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an  or  or  icon can be connected to target machines and have live links; all others will be inactive.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

**Note:** Users can disable remote control and FTP sessions by right-clicking the  icon on their managed machine and selecting **Disable Remote Control**. You can deny users this ability by removing **Disable Remote Control** using [Agent > Agent Menu \(page 73\)](#).

## ActiveX Control

An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package on a new machine, your browser may ask if it is OK to download and install this ActiveX control. Click yes when asked. If the ActiveX control is blocked by the browser from running, the user is presented with a link to manually download and run the remote control package manually.

## Helper Applications

In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the user machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the VSAuser machine and the remote machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

## Enable verbose relay

Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

## FTP the KServer

Clicking the [FTP the KServer](#) link starts an FTP session with the KServer itself. This option only displays for [master role users](#) (page 600).

## Enable / Disable the Machine User's Ability to Initiate FTP Remotely

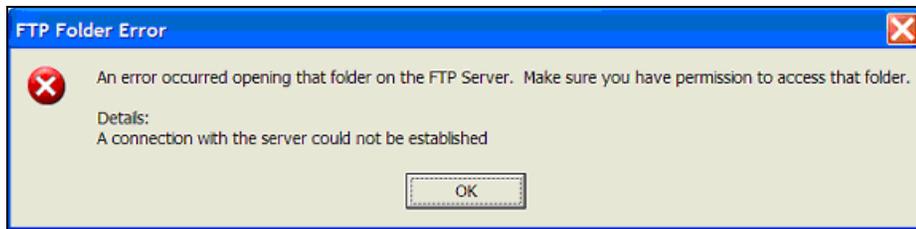
Users can enable / disable the machine user's ability to initiate FTP remotely to their own machine from another machine using Agent > [Portal Access](#) (page 81) and System > [Machine Roles](#) (page 403).

## FTP Malfunctions

Some reasons for FTP failure with managed machines are:

- The user machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Anti-virus software on the target machine may block the connection. This problem is eliminated if KES Security protection is installed on the target machine.
- Wrong primary KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using Agent > [Check-in Control](#) (page 75).
- You accessed the KServer from a different address. The helper application gets connection information from a cookie on the local machine. To access this information, the helper passes the URL of the KServer to Windows. Say you downloaded the helper application from `www.yourKServer.net`. Then you open a new browser and access the KServer by typing in its IP address `192.168.1.34`. The KServer drops a cookie for `192.168.13.34` while the helper tries to get a cookie corresponding to `www.yourKServer.net`. The helper won't find the cookie. If this happens to you, just download a new helper application and try again.
- FTP requires [Passive FTP](#) be turned **off**. If you get the following error after attempting an FTP session:

## Remote Control



Then disable **Passive FTP** on your browser as follows:

1. Open **Internet Options...** from IE's **Tools** menu.
2. Click on the **Advanced** tab.
3. In the **Browsing** section, look for **Use Passive FTP** and uncheck this setting.
4. Click OK and try FTP again.

## Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

## Machine.Group ID

The list of **Machine.Group IDs** (page 592) displayed is based on the **Machine ID / Group ID filter** (page 26) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 404).

## Enter a drive letter to FTP to

Enter the drive letter to FTP to, instead of selecting a remote fixed drive option.

**Note:** The KServer determines how many fixed disks a managed machine has via its **Latest Audit** (page 134).

---

# Task Manager

## Remote Control > Task Manager

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Task Manager** page performs the same function as Microsoft's Windows NT/2000 task manager. It lists all currently active processes on a managed machine. Clicking the link of a machine ID tasks the agent on the managed machine to collect 10 seconds of process data at the next check-in. **Task Manager** displays the results in tabular form. Task Manager supports all Windows operating systems, Windows 95 and up.

**Note:** You can also use **Live Connect** (page 380) to perform Task Manager tasks with a managed machine.

## kperfmon.exe

kperfmon.exe is a small program run by the agent to collect task data on the target machine. It only runs while collecting task data. On some OS configurations kperfmon.exe may take about 4% of the CPU during the 10 seconds required to collect data.

## Enable / Disable the Machine User's Ability to Access Task Manager Remotely

Users can enable / disable the machine user's access to Task Manager on their own machine remotely from another machine using the System > Machine Roles > [Access Rights](#) (page 403) tab

### Name

The name of the process actively running on the managed machine.

### CPU

The percent of CPU time consumed by that process over the 10 second data collection interval.

### Mem Usage

The amount of main memory used by each active process.

### Threads

The number of active threads associated with each active process.

### End Process

You can kill any active process on the managed machine by selecting the radio button to the left of the process name and then clicking the [End Process](#) button. In addition to killing the active process, it re-collects the task data again.

---

## Chat

### Remote Control > Chat

- This page applies to the following product: *On Premises*

The [Chat](#) page initiates or continues chat sessions with logged on users  on managed machines. Multiple chat sessions may be active at the same time. Each window title displays the machine ID name for that session. The system automatically removes all messages older than one hour. Press the [Shift-Enter](#) key combination to insert a carriage return into a message.

**Note:** You can also use [Live Connect](#) (page 380) to chat and video chat with a managed machine. Video chat allows you to video chat with anyone, not just a managed machine user.

### To Initiate a Chat Session

Click the machine ID of the machine you wish to start chatting with. A chat session window opens on your machine and a chat window opens in a browser on the remote machine. Enter text in the text pane. Click the [Send](#) button to send the message.

### To Respond to a Chat Session

If a chat popup window displays while you are logged on to the KServer, respond by entering text in the text pane. Click the [Send](#) button to send the message.

### Join Session link

Multiple VSA users may participate in the same chat session with a machine user. If a chat session is in

## Remote Control

progress, the [Join Session](#) link displays next to that machine ID. Click this link to join the session. **If the session was abnormally shut down**, click this link to restart the chat session and recover all messages for the session.

### Chatting with Other VSA Users

The names of [logged on](#) VSA users with [scope](#) (page 404) rights to the organizations and group IDs currently displayed by the [machine ID.group ID filter](#) (page 592) display on the [Chat](#) page as well. Click the link of another logged on VSA user to initiate a chat with that VSA user.

### Enable / Disable the Machine User's Ability to Initiate Chat with VSA Users

Users can enable / disable the machine user's ability to initiate a chat session with VSA users using the System > Machine Roles > [Access Rights](#) (page 403) tab.

### Ensuring Chat Opens a New Window

The default setting for [Internet Explorer](#) reuses open browser windows when any task opens a new URL. This same behavior occurs when you click a link in an email or Word document (the already open browser window is redirected to the new URL). To set Internet Explorer's default behavior to open new URLs in a new window perform the following steps:

1. Select [Internet Option...](#) from the [Tools](#) menu of any Internet Explorer window.
2. Click on the [Advanced](#) tab.
3. Uncheck the box labeled [Reuse windows for launching shortcuts](#) in the Browsing section.
4. Click [OK](#).

### My Machine Makes a 'Clicking' Noise Every Time the Chat Window Refreshes

Many Windows themes configure the system to play a sound every time Internet Explorer navigates to a new URL. One of these, `start.wav`, sounds like a click. To turn off the sound perform the following steps:

1. Open the [Control Panel](#) and select [Sounds and Multimedia](#).
2. Click on the [Sounds](#) tab.
3. Scroll down and select [Start Navigation](#) in the [Windows Explorer](#) section.
4. Select [\(None\)](#) from the drop-down control labeled [Name](#).
5. Click [OK](#).

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Play tone with each new message

Check this box to cause a tone to sound every time a new message is sent or received by a chat window.

### Automatically close chat window when either party ends chat

Check this box to close the chat window when either party ends the chat. Leave blank, if you want each party to be able to view and copy text from the chat window, even if the other party ends the chat.

### Remove your name from chat list seen by other administrators

Check this box to remove your name from the chat list seen by other VSA users.

### Remove your name from chat list seen by users

Check this box to remove your name from the chat list seen by machine users.

---

## Send Message

### Remote Control > Send Message

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The [Send Message](#) page sends network messages to selected machine IDs. Messages can be sent immediately at the next managed machine check-in, or can be scheduled to be sent at a future date and time.

The message either displays immediately on the managed machine, or the agent icon in the system tray of the managed machine flashes between a white background and its normal background when a message is waiting to be read. When the machine user click's the flashing icon the message displays.

Machine users can also be notified by a conventional Windows dialog box or through a browser window. If a browser window is used, enter a URL instead of a text message. This feature can be handy, for example, to automatically take users to a web page displaying an updated contact sheet or other relevant information.

**Note:** *Send and receive messages to and from other VSA users using [Info Center > View Dashboard](#) (page 180).*

### Enter message/URL sent to remote machines (dialog box or URL)

The text you enter depends on the display window you select.

- Enter a text message if the display window is a dialog box.
- Enter a URL if the display window is a browser.

### Select display window

Select the manner in which the user is notified on the managed machine. The default is `Dialog Box`, which displays a standard Windows dialog box with the network message. `Browser` displays a URL in a web browser window.

### Send Now

Click [Send Now](#) to send the message immediately to selected machines. The message displays in the [Messages Not Yet Sent](#) column until the message is received by the machine. For example, the machine may be offline.

## Remote Control

### Clear Messages

Click [Clear Messages](#) to remove messages that have not been delivered to managed machines.

### Schedule time to send message

Enter the year, month, day, hour, and minute to send the message.

### Schedule

Click [Schedule](#) to schedule delivery of the message to selected machine IDs using the schedule options previously selected. The message displays in the [Messages Not Yet Sent](#) column until the message is received by the selected machine.

### Display Immediately/Flash Icon

This setting determines how managed machine users are notified once their message has been retrieved from the KServer.

- [Display Immediately](#) notifies the user immediately.
- [Flash Icon](#) flashes the agent icon in the [system tray](#) (on page 599) until the user clicks the icon. The message is then displayed according to the settings in [Select display window](#).

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

### Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Machine.Group ID

The list of [Machine.Group IDs](#) (page 592) displayed is based on the [Machine ID / Group ID filter](#) (page 26) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 404).

### Current User

Displays the currently logged on user.

### Messages Not Yet Sent

This column displays messages not yet sent.

---

# Power Management

## Remote Control > Power Management

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Power Management** page powers on, powers off or reboots vPro-enabled machines. Power management options are executed using the agent of the managed machine that originally identified the vPro-enabled machine using **LAN Watch** (page 56). A **vPro** (page 600) credential is required to execute power management options on a vPro-enabled machine. You can specify a credential using this page.

**Note:** You can display the hardware assets of vPro-enabled machines with credentials using **Agent > View vPro** (page 69).

This page provides you with the following actions:

**Schedule** - Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
  - **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
  - **Power up if offline** - If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
  - **Exclude the following time range** - If checked, specifies a date/time range to not perform the task.
- **Run Now** - Run the power management options now on selected machine IDs.
  - **Cancel** - Cancel schedule options for selected machined IDs.
  - **Power Up / Power Down / Reboot** - Select the power management option to execute.

## Expand / Collapse

Click the plus icon of a vPro machine ID to display a history table of power management actions performed on that machine. Click the minus icon to collapse the history table.

### Type

The power management option scheduled to be executed.

### Last Power Management

The last time a power management option was executed.

### New Power Management

The next time a power management option is scheduled to be executed.

## Machine ID. Group ID

The machine ID.Group ID of this vPro-enabled machine, if an agent is installed. Blank, if no agent is installed.

## vPro Host Name

The name for the vPro-enabled machine set by vPro configuration.

## Remote Control

### Proxy Agent

The machine ID.group ID of another managed machine used to execute power on, power off or reboot this vPro-enabled machine. The [Proxy Agent](#) must be on the same LAN as the vPro machine.

### OS Computer Name

The name for the vPro-enabled machine set by the operating system.

### IP Address

The IP address of the vPro-enabled machine.

### Credentials

A vPro credential is typically collected during a [LAN Watch](#) scan. A credential is required by the vPro machine to respond to both [Power Management](#) and [Remote ISO Boot](#) (*page 378*) requests. If no credential exists or the credential needs to be changed you can click this cell to enter a new credential.

---

## Remote ISO Boot

### Remote Control > Remote ISO Boot

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Remote ISO Boot](#) page boots [VPro](#) (*page 600*) machines from an ISO image. An agent machine on the same LAN as the target vPro machine is used to mount a virtual disk on the VPro machine. The virtual disk points to a UNC share on the LAN containing an ISO image. The agent machine then boots the VPro machine from the virtual disk. A [Remote ISO Boot](#) cannot be scheduled. The boot occurs immediately.

**Warning:** Kaseya does not provide ISO images and is not responsible for 100% automation of the boot. A boot may require a user to hit any key to boot from ISO image, else the boot might occur from the hard drive.

### VPro Configuration Requirements

- The agent cannot be on the vPro machine. It has to be on a different machine in the same LAN.
- The VPro machine being booted must be VPro 3.0 or greater.
- SOL/IDE-R must be enabled in the Intel AMT BIOS extension. This cannot be done remotely.
- The agent machine used to boot the vPro machine, the VPro machines being booted and the UNC must all be on the same LAN.
- Only UNC shares can be specified. Mapped drives are not allowed.
- Credentials must be defined in advance, providing access to:
  - The agent machine - Use Agent > [Set Credential](#) (*page 83*) if necessary.
  - The UNC share on the LAN - The network credentials and UNC are both specified when the ISO boot icon is clicked in the [Remote ISO Boot](#) grid.
  - The vPro machine - vPro credentials are configured either during [LAN Watch](#) (*page 56*) scan or by clicking on the credentials icon in the [Remote ISO Boot](#) or [Power Management](#) grid.

### Host Name

The name for the vPro-enabled machine set by vPro configuration.

## Proxy Agent

The machine ID.group ID of another managed machine used to execute power on, power off or reboot this vPro-enabled machine. The **Proxy Agent** must be on the same LAN as the vPro machine.

## Machine.Group ID

The machine ID.group ID of this vPro-enabled machine, if an agent is installed. Blank, if no agent is installed.

## Credentials

The vPro credentials are typically collected during a **LAN Watch** scan. The credentials are required by the vPro machine to respond to both **Power Management** (*page 377*) and **Remote ISO Boot** requests. If none are defined or they need to be changed you can click this cell to define a new credential.

## Remote ISO Boot

Click the **Remote ISO Boot** icon to specify the **UNC File Path**, **User Name** and **Password**. Then click the **Go** button.

- The **UNC File Path** must include the filename of the ISO image.
- The **User Name** and **Password** is required to access to the ISO image file on the LAN.

## Components

ISO boot is implemented via the following components:

- `VProProxy.dll` - This dll is used by the agent on the agent machine to communicate with the VPro machine.
- `Redirect.exe` - This process is run with the passed in network credentials and manages the virtual drive.

## Switches

The following are switches sent to `VProProxy.dll` when doing an ISO boot.

- `-redirect` - We're going to do a redirect operation. Possible values - command
- `-username` - The VPro user name (like admin)
- `-password` - The password for the VPro user
- `-ip` - The ip address of the target machine
- `-iso` - The UNC path to the ISO image
- `-redirectPath` - The path to `redirect.exe`
- `-o` - The full name and path of the out file for `VProProxy.dll`
- `-redirectOut` - The full name and path of the out file for `redirect.exe`
- `-netUsername` - The name of the network user with authority to access iso image. Name must be in the form of `name@domain`.
- `-newPassword` - The password for the network user

## Example

The following is an example of a command line using the switches above.

```
C:\temp\VProProxy.dll -redirect command -username admin -password Pass=W0rd
-ip 10.10.10.58 -iso "\\10.10.10.139\ISOImages\EN_WINDOWS_XP_PRO_WITH_SP2.ISO"
-redirectPath C:\temp\redirect.exe -o C:\temp\ProxyOut.txt
-netUsername john.smith@kaseya.com -netPassword SomePassword
-redirectOut c:\temp\RedirectInfo.txt
```

## Live Connect

### Live Connect

The **Live Connect** page displays by *clicking any check-in icon, for example* , next to any machine ID in the VSA.

**Live Connect** enables you to perform system level tasks and functions on a single managed machine, in most cases without having to interrupt the user.

**Note:** The *first* time **Live Connect** launches from any machine, it asks to install several browser plugins.

### Windows

Live Connect for Windows machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**, **File Manager**, **Command Shell**, **Registry Editor**, **Task Manager**, **Event Viewer**, **Ticketing**, **Chat**, **Desktop Access** and **Video Chat**.

### Macintosh

**Live Connect** for Macintosh machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**, **Ticketing**, **Chat**, **Desktop Access** and **Video Chat**. Does not include a thumbnail preview image of the desktop in **Live Connect**.

**Note:** On Mac Leopard (Intel) systems, you can use **Desktop Access** in **Live Connect** to remote control a Windows system using Firefox, Safari, or Chrome. On Windows systems using any of our supported browsers you can use **Desktop Access** to remote control a Mac Leopard (Intel) system.

### Window Header

Basic information about the managed machine displays at the top of the **Live Connect** window.

- **Thumbnail View** - The desktop of the currently logged on user displays in a thumbnail view, if a user is logged onto the machine.
- **Machine Info** - Lists basic information about the managed machine.
- **Performance Graphs** - Shows CPU % and Memory % performance graphs for the managed machine.
- **Log Off** - Only displays if a machine user using **Portal Access** is logged in remotely from the machine.
- **Help** - Displays online help for **Live Connect**.

### Menu Options

A menu of tabbed property sheet provides access to various categories of information about the managed machine.

- **Home** - *The **Home** tab is the first tab displayed when the **Live Connect** window opens.*
  - **Home** - Typically the **Home** tab displays a welcome message and the URL page of the agent service provider. The **Run Procedures** section of the **Home** tab enables the **Live Connect** user to run agent procedures on the managed machine immediately. A **Custom Links** section may display on the **Home** tab, if specified by the service provider, offering links to additional resources. Multiple customized **Home** tabs are possible, each with a unique name, if specified by the service provider.
  - **Change Logon** - Changes the *remote* logon user name and password for this managed machine. These logon options enable a user to access the **Live Connect** window to this managed machine from any other machine, including initiating a remote desktop session with the managed machine, if **Desktop Access** is enabled by the service provider. Enter the same URL used to logon to the VSA. Then enter the **Live Connect** user name and password specified in this tab. Accessing **Live Connect** remotely in this manner from another machine is

called **Portal Access**. **Portal Access** logon options can also be maintained within the VSA using Agent > **Portal Access** (page 81).

- **Change Profile** - Changes the contact information for this managed machine. This information populates a ticket with contact information when **Live Connect** is used to create a ticket. This information can also be maintained using Agent > **Edit Profile** (page 79).
- **Agent Data** - Displays the following tabs:
  - **Pending Procedures** - Displays and schedules pending agent procedures for a managed machine and the agent procedure history for that machine. Includes the execution date/time, status and user who scheduled the procedure.
    - ✓ Click the **Schedule Another Procedure** button to schedule a procedure not yet pending. Once selected and scheduled, the procedure displays at the bottom of the **Pending Procedures** section.
    - ✓ Click the **Schedule** button to schedule a selected procedure to run in the future or on recurring basis.
    - ✓ Click the **Run Now** button to run a selected procedure once immediately.
    - ✓ Click the **Cancel** button to cancel any selected pending procedure.
  - **Logs** - Displays the logs available for a machine: Alarm Log, Monitor Action Log, Agent Log, Configuration Changes, Network Statistics, Event Log, Agent Procedure Log, Remote Control Log, Log Monitoring.
  - **Patch Status** - Displays **Missing** and **Pending** Microsoft patches and schedules missing patches. If a machine belongs to a **patch policy** (page 595), missing patches may be further identified as **Denied (Pending Approval)**. The user can manually override the denied patch policy by scheduling the patch.
    - ✓ Click the **Schedule** button to schedule a selected missing patch.
    - ✓ Click the **Cancel** button to cancel a selected pending patch.
    - ✓ Click the **Show History** link to display the history of patches installed on the managed machine.
  - **Agent Settings** - Displays information about the agent on the managed machine:
    - ✓ **Agent version**
    - ✓ **Last check-in**
    - ✓ **Last reboot**
    - ✓ **First time check-in**
    - ✓ **Patch Policy Membership** - Defined using Patch Management > **Membership: Patch Policy** (page 327)
    - ✓ **View Definition Collections** - Defined using the **Only show selected machine IDs** option in **View Definitions** (page 28).
    - ✓ **Working Directory** - Can also be defined using Agent > **Working Directory** (page 78).
    - ✓ **Check-In Control** - Can also be defined using Agent > **Check-In Control** (page 75).
    - ✓ **Edit Profile** - Can also be defined using Agent > **Edit Profile** (page 79).
    - ✓ **Agent Logs and Profiles** - Can also be defined using Agent > **Log History** (page 35).
  - **Documents** - Lists documents uploaded to the KServer for a managed machine. You can upload additional documents. Provides the same functionality as Audit > **Documents** (page 143).
  - **Get File** - Accesses files previously uploaded from a managed machine. Click the link underneath a file to display the file or run it. Provides the same functionality as Agent Procedures > **Get Files** (page 127).
- **Audit Information** - Information tabs include: **Machine Info**, **Installed Applications**, **System Information**, **Disk Volumes**, **PCI & Disk Hardware**, and **Printers**. Provides audit information based on your **Latest Audit** (page 587). You can perform an an immediate audit using the **Machine Info** tab.

## Remote Control

- **File Manager** - Displays two file managers, one for your local machine and one for the managed machine. Using the *upper panes* only you can:
  - Create directories and delete, refresh or rename files or directories using either file manager.
  - *Move* files within the *same* file manager using drag and drop.
  - *Copy* files *between* file managers using drag and drop.
- **Command Shell** - Opens a command shell on the managed machine. Defaults to the `c:\windows\system32` directory.
- **Registry Editor** - Displays the registry of the managed machine ID. You can create, rename, refresh or delete keys and values, and set the data for values.
- **Task Manager** - Lists Windows Task Manager data for the managed machine. You can stop or prioritize **Processes**, stop and start **Services**, check typical **Performance** benchmarks for each process, categorized by CPU, disk, network, and memory, review **Users** session data, **Reboot**, power off the managed machine, or log off sessions on the managed machine, and display **User and Groups** on the managed machine.
- **Event Viewer** - Displays event data stored on the managed machine by event log type.
- **Ticketing** - Displays and creates tickets for the managed machine. Displays and creates tickets for **Ticketing** module tickets or tickets and knowledge base articles for the **Service Desk** module, depending on which module is activated.

**Note:** A service desk must be a member of the `Anonymous` scope to display **Service Desk** tickets in a machine user **Portal Access** session of **Live Connect**.

- **Chat** - Initiates a chat session with the currently logged on user of the managed machine. You can invite other VSA users to join your chat session. See Remote Control > **Chat** (page 373) for more information.
- **Desktop Access** - Initiates a remote desktop session with the managed machine.
  - **Share session using VNC** - Use VNC to connect to the desktop.
  - **Create a private session using RDP** - Use RDP to connect to the desktop.
  - **Connect to printers** - If checked, desktop access includes access to printers.
  - **Connect to mapped drives** - If checked, desktop access includes mapped drives.
  - **Automatically connect with saved settings** - If checked and a desktop session has been saved, then **Desktop Access** connects immediately using the previously saved settings when:
    - ✓ Clicking the **Desktop Access** menu item in **Live Connect**
    - ✓ Clicking **Desktop Access** using the **agent quick view** (page 583) window.
  - **Display the connection** - Options include `Embedded in this window`, `in a new window`, `as full screen`.
  - **Automatically hide Live Connect panels** - Options include `Top Panel`, `Left panel`, `Both Panels`.
  - **Reset Warnings** - Show warnings about active sessions. - Only one **Desktop Access** session is supported for each **Live Connect** session. If clicked and a **Desktop Access** is active in a separate window, a warning box displays in the **Live Connect** session to warn you that a **Desktop Access** session is active in another window.
- **Video Chat** - If a machine user is logged on to a managed machine, then a **Live Connect** user can initiate a audio/video chat session with that logged on machine user. The session can be audio only for one or both machines if video is not supported on one or both machines.
  - **Video Chat with the Machine User** - Click the Call button to initiate the video chat session. The machine user will see a browser window or browser tab display on their machine that lets them see your video image and their own video image if their machine has a webcam installed.
  - **Video Chat with Anyone** - Click the Connect URL button. This copies a URL to your clipboard. Copy the URL address into any email or instant message program and send it to anyone.

When that URL is entered in a browser the individual will be able to video chat with you. *Video chat does not require the person receiving the chat invitation to be a managed machine.*

- **Video Chat Confirmation** - The Adobe Flash Player used to transmit the audio/video stream requires each user click an "Allow" button to proceed with their side of the video chat.
- **Audio/Video Controls** - Hover the mouse over either video image in the chat window to display audio/video controls.
- **Text Chat** - You can text chat and video chat at the same time using the same window.
- **Anti-Malware** - Displays the Anti-Malware status of the managed machine, if installed.
- **Anti-Virus** - Displays the Antivirus status of the managed machine, if installed.
- **Discovery** - Displays the Network Discovery status of the machine, if installed.

## Additional Notes

- Access to specific **Live Connect** functions depends on access rights in System > User Roles > **Access Rights** (page 401) and Machine Roles > **Access Rights** (page 403).
- All of the **Live Connect** menu options are enabled when the machine is connected to **Live Connect**. Only **Home**, **Audit Information**, **Agent Data** and **Ticketing** are enabled when the machine disconnected from **Live Connect**.
- You can customize the **Live Connect Home** page using System > Customize: **Live Connect** (page 432).
- **Event Viewer** data does not depend on Agent > **Event Log Settings** (page 37).
- If a `externalLink.xml` exists in the `\Webpages\install` directory of the KServer a **New Ticket** link displays next to the **Help** link in **Live Connect**. Clicking the **New Ticket** link redirects users to the URL specified in `externalLink.xml`. See **Customized New Ticket Link** (page 383) for details.

## Customized New Ticket Link

To customize **New Ticket** links on the **Live Connect** page, fill out the `externalLink.xml` file as described in the comments section of the XML below. To activate the new ticket link, place the `externalLink.xml` file in the `\WebPages\install\` directory of your KServer.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
  machineNameVal - the machine name for the active machine is substituted
                   in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
  url="http://192.168.212.52/?mname=machineNameVal&gname=groupNameVal"/>
</externalLinks>
```



## Chapter 10

# System

### In This Chapter

System Overview	387
User Settings	391
System Preferences	393
User Security	397
Orgs/Groups/Depts/Staff	408
Server Management	412
Customize	428

## **System**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# System Overview

## System

The **System** module enables users to maintain policies for the entire system:

- **Preferences**
- **User Security**
- **Organizations, Groups, Departments and Staff**
- **Server Management**
- **Customization**
- **Database Views**

---

<b>Functions</b>	<b>Description</b>
<b>Preferences</b> (page 391)	Sets system-wide preferences that apply only to the currently logged in user.
<b>Change Logon</b> (page 392)	Changes the username, password and security question of the currently logged on user.
<b>Check-in Policy</b> (page 393)	Set limits on a variety of agent check-in parameters.
<b>Naming Policy</b> (page 395)	Automatically enforces naming policies based on each machines IP address, network, and computer name
<b>Users</b> (page 397)	Creates, edits and deletes users.
<b>User Roles</b> (page 400)	Creates and deletes user roles. User roles determine the access rights for VSA users. Assign roles types to user roles.
<b>Machine Roles</b> (page 403)	Creates and deletes machine roles. Machine roles determine the access rights for machine users. Assign role types to machine roles.
<b>Scopes</b> (page 404)	Assigns organization, machine groups, machines, departments and service desks to scopes.
<b>Logon Hours</b> (page 407)	Specifies when users can logon to the VSA.
<b>User History</b> (page 408)	Displays the functions visited in the last 30 days for each user.
<b>Manage</b> (page 408)	Defines organizations, groups, departments and staff members of departments.
<b>Set-up Types</b> (page 411)	Defines types of organizations.
<b>Request Support</b> (page 412)	Accesses Kaseya support.
<b>Configure</b> (page 412)	Displays KServer information, license code and subscription information, obtains latest server updates, and server IP information.
<b>License Manager</b> (page 420)	Allocates available agent and user licenses.
<b>System Log</b> (page 423)	Logs events that can not be tracked by machine ID.
<b>Statistics</b> (page 423)	Displays VSA server performance statistics
<b>Logon Policy</b> (page 425)	Sets user logon policies.
<b>Application Logging</b> (page 426)	Enables or disables logging of application-layer transactions. Typically used only by Kaseya support.
<b>Outbound Email</b> (page 426)	Defines the email server for outbound email.

---

## System

<a href="#">Color Scheme</a> (page 16)	Determines the set of colors displayed by the VSA environment for the current user.
<a href="#">Site Customization</a> (page 428)	Customizes the user interface for all users. <ul style="list-style-type: none"><li>• Logon Page</li><li>• Site Header</li><li>• Report Header</li><li>• Agent Icons</li></ul>
<a href="#">Live Connect</a> (page 432)	Customizes the Live Connect home pages seen by VSA users and machine users.
<a href="#">Database Views</a> (page 472)	Configures database view access.

## VSA Logon Policies

Once a VSA user is defined in System > [User Security](#) (page 397), a number of functions manage when and how users can logon and the features that are available to them during logon.

VSA user logon options are specified using:

- System > [Users](#) (page 397) - Optionally reset the user's password, or force the user to change his or her password, or enable/disable the user's logon or log a user off.
- System > [Preferences](#) (page 391) - The [Preferences](#) page sets preference options that typically apply *only to the currently logged in user*.
- System > [Change Logons](#) (page 392) - The [Change Logon](#) page sets your VSA logon username and password. These preference options apply *only to the currently logged on user*.
- System > [Logon Policy](#) (page 425) - The [Logon Policy](#) page sets logon policies that apply to all VSA users.
- System > [Logon Hours](#) (page 407) - The [Logon Hours](#) page determines *when* users can logon to the VSA by specifying the weekdays and hours for each user role. Each day of the week can have different hours of operation set.
- System > Site Customization > [Logon Page](#) (page 428) - Set options that display on the logon page.
- System > Site Customization > [Site Header](#) (page 429) - Set options that display on the logon page.

**Note:** Additional logon options *for machine users only* are set in Agent > [Portal Access](#) (page 81).

**Note:** See [Embedding the VSA Logon Form in Web Pages](#) (page 388).

## Embedding the VSA Logon Form in Web Pages

You can embed the VSA logon form in web pages.



Enter Your Username and Password

Username

Password

Remember my username on this computer

Include the following HTML code, replacing the `server.name` text with the name of your VSA.

```
<iframe src="http://server.name/access/logon.asp?embedLogon=true"  
name="getChallenge" scrolling="no" frameborder=0 width=280 height=250  
marginwidth=0 marginheight=0 />
```



## User Settings

**User Settings** pages set options that typically apply *only to the currently logged on user*.

### Preferences

#### System > Preferences

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Preferences** page sets system-wide preferences that apply *only to the currently logged on user*. This includes the email address where you receive alert messages.

**Note:** Three options on this page apply to *all users* and only display for master role users: setting the **System Default Language Preference** and the **Download** button for installing language packs, and **Show shared and private folder contents from all users**.

**Note:** See **VSA Logon Policies** (page 388) for a summary of functions affecting user logons.

#### Set email address to deliver messages for this administrator to

Specifies the email address that alerts, ticket notifications and other email messages will be sent to. After entering the email address, click **Apply** to make it active. Previously set alerts retain the original email recipient addresses specified when the alerts were set.

#### Set first function after logon

Select the name of the function you want to see when you first log on to the KServer.

#### Set delay before displaying detail information when hovering over information icon

A  information icon displays for each ticket row in Ticketing > **View Summary** (page 435) and Service Desk > Tickets. Hovering the cursor over the icon displays a preview of the ticket. Specify the number of milliseconds to wait before the ticket preview window displays, then click the **Apply** button. Click the **Default** button to set this value back to its default.

#### Set delay before displaying detail information when hovering over agent icon

An agent check-in icon, for example , displays next to each machine ID account in the VSA. Hovering the cursor over the icon displays an **agent quick view window** (page 583). Specify the number of milliseconds to wait before the agent quick view window displays, then click the **Apply** button. Click the **Default** button to set this value back to its default.

#### Select time zone offset

Select one of the following time zone offset options, then click **Apply**.

- **Use time zone of the browser logging into the system**
- **Use time zone of the VSA server** - The time currently being used by the VSA displays next to this option.
- **Use fixed offset from the VSA server <N> hours**

**Note:** Date format is set in System > Configure (page 412).

## Set up language preferences

- **My language preference is** - Select the language you prefer displayed when you're logged into the KServer. The languages available depend on the language packs installed.
- **System default language preference is** - Select the default language used by the VSA user interface for all users. The languages available depend on the language packs installed. This option only displays for **master role users** (page 600).
- **Download a Language Pack** - Display a dialog box that enables you to download and install language packs. A language pack enables the VSA user interface to be displayed in that language. This option only displays for **master role users** (page 600).

## Show shared and private folder contents from all users - Master Admin Only

If checked, a master role user has visibility of all shared and private folders. For private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

**Note:** A master role user can get all access rights to any shared folder by taking ownership.

## Select display format for long names

The web pages are designed to display well for typical string sizes. Occasionally data fields contain long names that will not display properly on the web pages. You can specify how long names display as follows:

- **Limit names for better page layout** - This setting limits the string size to fit well on the web page. Strings exceeding a maximum length are limited with a ... To view the entire name, hover the mouse over the string and a tool tip pops up showing the entire name.
- **Allow long name wrapping** - Long strings are allowed to wrap within the web page. This may disturb the normal web page layout and names may wrap at any character position.

## Clear Snooze

Click **Clear Snooze** to clear all outstanding task notification messages. Task notification messages are generated for tasks that are assigned to you and for tasks that are past due. Tasks are defined using the InfoCenter > **View Dashboard** (page 180) page.

## Defaults

Click **Defaults** to reset all settings to system defaults for this user.

## Change Logon

### System > Change Logon

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Change Logon** page sets your VSA logon username and password. These preference options apply *only to the currently logged on user*.

**Note:** See **VSA Logon Policies** (page 388) for a summary of functions affecting user logons.

## Changing Your VSA Logon Name and/or Password

To change your logon name and password:

1. Enter a new name in the **Username** field.

**Note:** The **Username** field cannot be edited if **Prevent anyone from changing their logon** is checked in **System > Logon Policy**.

2. Enter your old password in the **Old Password** field.
3. Enter a new password in the **New Password** field. Passwords are case-sensitive.

**Note:** If you would like the system to generate a strong password for you, click **Suggest**. A dialog box displays showing the new password; the new password is automatically entered in the **New Password** and **Confirm Password** fields. Be sure to write it down before clicking **OK** and closing the dialog box.

4. Confirm the password by re-typing it in the **Confirm Password** field.
5. Enter a **Security Question** and **Security Answer**.

**Note:** Clicking the **Forgot Password?** link on the logon page—if activated using the **System > Site Customization > Logon Page** (page 428) tab—emails you a link where you can change your password. To change your password, you must have already filled out a **Security Question** and **Security Answer** using **System > Change Logon** (page 392).

6. Click **Change**.

### Converting Your Existing VSA Logon to use your Domain Logon

You can convert your own VSA logon to use your domain logon as follows:

1. Open the **System > Change Logon** page in the VSA.
2. Enter your current VSA password in the **Old Password** field.
3. Enter you domain and domain logon name, formatted *all in lowercase* using the format `domain/username`, in the **Username** field.
4. Enter your domain password in the **New Password / Confirm Password** fields.

This enables you to logon to the VSA using your domain logon and have your VSA logon name and password managed using Active Directory. At the same time, you can continue to use all your previous VSA share rights, procedures and other user settings.

**Note:** If a VSA user logon is based on an AD user, the VSA user's username and password cannot be changed within the VSA, only in Active Directory. Once usernames and passwords are changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep VSA logons updated with the latest changes to AD logons. See **Agent > View AD Users** (page 66) for more information.

---

## System Preferences

### Check-in Policy

#### System > Check-in Policy

- This page applies to the following product: *On Premises*

The **Check-in Policy** page defines group ID policies controlling the minimum, maximum and fixed values allowed for a variety of options. These policies prevent users from selecting settings that place undue stress on Windows servers running the KServer.

### Changing One Field at a Time

If you need to make a change to only one setting in a group:

1. Enter a new value in the field you want to change.
2. Leave all other fields empty. This indicates that these fields will remain unchanged.

## System

3. Click **Update**.

### Min/Max Age for Log Entries

These values determine the minimum and maximum values that can be entered in the **Set Max Age for Log Entries** options in Agent > **Log History** (page 35). To remove a value, enter 0 (zero).

### Check-In Period

These values determine the minimum and maximum settings that can be entered in the **Check-In Period** setting of Agent > **Check-In Control** (page 75). To remove a value, enter 0 (zero).

### KServer Address (0 for editable) - Primary/Second

If 0 is entered in the **Primary** or **Secondary** fields and **Update** clicked, then the **KServer (1st) (2nd)** column of selected group IDs displays `Editable`. Users can enter any domain name server (DNS) name or IP address they like in the **Primary KServer** and **Secondary KServer** fields in Agent > **Check-in Control**.

If these checkboxes are checked and *DNS names or IP addresses are entered* in these fields and **Update** clicked, the **KServer** column of selected group IDs display fixed DNS names or IP addresses. Users are required to use these fixed IP addresses in the **Primary KServer** and **Secondary KServer** fields in Agent > **Check-in Control**.

**Best Practices:** Although a public IP address may be used, Kaseya recommends using a domain name server (DNS) name for the KServer. This practice is recommended as a precaution should the IP address need to change. It is easier to modify the DNS entry than redirecting orphaned agents.

### Allow automatic account creation for selected Group ID

If enabled, new machine ID accounts are created automatically for selected group IDs as soon as the machine's agent checks into the KServer the first time using a new machine ID name and selected group ID.

For example, an agent is installed on a new machine. The group ID `acme` already exists, but the machine ID `ksmith` does not. With this option enabled for the `acme` group ID, the `ksmith.acme` machineID.group ID account is created as soon as the agent checks in the first time.

**Note:** Allow automatic account creation for selected Group ID is enabled by default.

To enable automatic account creation for selected group IDs:

1. Check **Allow automatic account creation for selected Group ID**.
  2. Select group IDs in the paging area.
  3. Click **Update**.
- `Auto Enabled` displays in the **Group IDs/Auto Acct** column of selected group IDs.

### Allow automatic account creation for groups without a policy

This option only displays for **master role users** (page 600). If enabled, new machine ID accounts are created automatically for group IDs that do not have any **Check-in Policy** defined, or for agents with a group ID that does not yet exist, as soon as the machine's agent checks into the KServer the first time using a new machine ID name.

**Note:** Allow automatic account creation for groups without a policy is enabled by default.

## Update

Click **Update** to apply policy parameters to selected group IDs.

## Remove

Click [Remove](#) to remove policy parameters from selected group IDs.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Groups IDs

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

## Auto Acct

`Auto Enabled` indicates automatic account creation is enabled for this group ID.

## Log Age (Min) / Log Age (Max)

Lists the settings entered in the [Set Max Age For Log Entries](#) fields in the header, for each group ID.

## KServer (1st) (2nd)

Lists the IP addresses/host names of the primary (1st) and secondary (2nd) servers allowed for group IDs.

## Check-in (Min) / Check-in (Max)

Lists the settings entered in the [Check-In Period](#) fields in the header, for each group ID.

## Naming Policy

### System > Naming Policy

- This page applies to the following product: *On Premises*

The [Naming Policy](#) page defines the IP address criteria used to automatically re-assign machines to a different machine group. Each machine group can be assigned multiple naming policies.

Naming policies can also force the renaming of a machine ID, if the machine ID name doesn't match the computer name, reducing confusion when administering managed machines.

Assigning machines to machine groups by IP addresses has the following benefits:

- Typically an organization represents a single customer enterprise and group IDs and subgroups represent locations within that enterprise. When an employee transfers to a new location, the managed machine can be automatically re-assigned to the appropriate machine group or sub-group for that location as soon as the managed machine's agent checks in from the new location's network.
- Using [managed variables](#) (*page 117*), managed machines can run procedures that access *locally available resources* based on the group ID or subgroup ID. Using [Naming Policy](#) this benefit can be applied automatically by IP address even to a highly mobile workforce that travels between different enterprise locations.
- Maintaining multiple agent install packages in Agent > [Deploy Agents](#) (*page 39*), one for each organization, can be time consuming. Instead some server providers use a single agent package for the `unnamed` organization and perform all installs using this package. System > [Naming Policy](#) (*page 395*) can reassign new agents to the correct organization.group ID automatically—the first time the agents check in—based on each managed machine's IP or connection gateway. Agent > [Copy Settings](#) (*page 70*) may be used afterwards, to manually copy specific kinds of agent settings by [machine ID template](#) (*page 592*) to the type of machine revealed by the initial audit.

## System

### Connection Gateway

Optionally check the **Connection Gateway** checkbox and enter the connection gateway IP address. The connection gateway is typically the WAN address of the managed machine. This rule can be applied independently to a group ID. The managed machine must have this IP address as its connection gateway to be automatically assigned to the group ID.

### IP Range

Optionally check the **IP Range** checkbox and enter an IP address range, such as 192.168.1.2 – 192.168.1.254. This rule can be applied independently to a group ID. The IP address of the managed machine must fall within this range to be automatically assigned to the group ID.

### Force machine ID to always be computer name

Optionally check the **Force machine ID to always be computer name** checkbox to force each machine ID name to match its corresponding computer name. This rule can be applied independently to a group ID.

**Note:** Machines are renamed to the new group ID at their next full check-in (page 588). The quick check-in (page 588) cycle does not trigger a rename. To rename a group of machines quickly using Naming Policy, schedule the Force Check-in sample agent procedure located in Agent Procedures > Schedule / Create (page 94).

### Update

Click **Update** to apply the naming policy to the selected machine group. The system immediately begins enforcing the group ID's new rule as machines check into the KServer.

### Add

Click **Add** to add a new naming policy to existing naming policies for a selected machine group.

**Note:** Each machine group can be assigned multiple naming policies. Use this capability to automatically assign machines with different IP address ranges to the same machine group.

### Clear

Click **Clear** to remove the naming policy from a machine group. The system immediately stops applying the rule for the machine group.

### Machine Group

This column lists the machine groups defined for the system. Select the radio button beside a **Machine Group** before updating, adding or clearing a naming policy.

### Connection Gateway

Displays the connection gateway assigned to the machine group.

### IP Range

Displays the IP ranges assigned to the the machine groups.

### Force Machine ID

Displays a check mark if **Force machine ID to always be computer name** is enabled for a machine group.

# User Security

## System > User Security

**User Security** determines the access users have to functions and data objects within the VSA. Understanding **User Security** configuration is easiest if you consider each of the following concepts in the order presented.

1. **Scope Data Objects** (page 408) - A **data object** is an object that you create and name. An example of a data object is a machine group. Some data objects are significant enough to be managed by scopes. Scope level data objects are defined *first*, before being assigned to scopes. Scope data objects include organizations, machine groups, machines, departments and service desks.
2. **Scopes** (page 404) - Sets of data objects that users have *visibility* of within the VSA.
3. **User Roles** (page 400) - Sets of VSA functions that VSA users can perform. A **function** acts on data objects. Examples of functions are opening, adding, editing or deleting records.
4. **User Role Types** (page 402) - Built-in classifications that determine the types of *user-role-based* licenses to apply to users in user roles.
5. **Machine Roles** (page 403) - Sets of **Portal Access** (page 81) functions that machine users can perform when displaying the VSA **Portal Access** page on their machine.
6. **Machine Role Types** (page 404) - Built-in classifications that determines the type of *machine-role-based* licenses to apply to machines in a machine role.
7. **Users** (page 397) - Refers to VSA users. Users of machines with agents on them are always identified as *machine users* to distinguish them from VSA users.

## Users

### System > User Security > Users

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Users** page creates and deletes user accounts. This page can also assign users to **User Roles** (page 400) and **Scopes** (page 404) when the user account is created.

### Users

Each user must be assigned at least one role and one scope. You can assign multiple roles and scopes to a user, but *only one role and one scope is active at any one time*. The active role and scope are selected using the **Role** and **Scope** drop-down lists in the top-right corner of the page. You can reset the user's password, enable/disable user logons and log off users if you have access to these functions.

**Note:** See **Master Users vs. Standard Users** (page 399).

**Note:** Each user can change their own logon name, password and email address using **System > Preferences** (page 391).

**Warning:** To simplify management and auditing of your VSA, provide each user with their own unique logon name. Avoid using generic logons like **User** or **Admin**. Generic logons make it difficult to audit the administrative actions taken by each user.

### Creating a New User

1. Click **New**. The **Add User** dialog box displays.
2. Enter **User Information**:

## System

- Enter a **Email Address** for the new user.
  - Select an **Initial Role** for new user.
  - Select an **Initial Scope** for the new user.
  - Enter a **First Name** and **Last Name**.
3. Optionally enter **Related Org Staff Member** information:
    - Select a **Staff Org**.
    - Select a **Staff Dept**.
    - Enter or select a **Staff Member**.
  4. Define **User Credentials**:
    - Enter a **User Name**.
    - Enter a password in the **Password** and **Confirm Password** fields. Passwords are case-sensitive.

**Note:** If you would like the system to generate a strong password for you, click **Suggest**. The new password is automatically entered in the **Password** and **Confirm Password** fields. Be sure to write it down before clicking **OK** and closing the dialog box.

    - Check the **Require password change at next logon** checkbox to force the user to enter a new password when they first logon.
  5. Click **Save**. The new user displays in the middle pane.

## Changing an Existing User Record

1. Click a **User** displayed in the middle pane.
2. Optional **Edit** the following attributes of the User record:
  - **First Name**
  - **Last Name**
  - **Email Address**
  - **Staff Org**
  - **Staff Dept**
  - **Staff Member**
3. Optionally add or remove roles using the **Roles** tab.
4. Optionally add or remove scopes using the **Scopes** tab.
5. Optionally change the password by clicking the **Set Password** button.
6. Optionally force a user to change their password by clicking the **Force Password** button.
7. Optionally enable / disable user logons by clicking the **Enable** or **Disable** buttons.

## Set Password

Select a user in the middle pane and click **Set Password** to change the password for the selected user. Passwords are case-sensitive.

## Force Password

Forces a selected user in the middle pane to change their logon the next time they logon.

## Enable / Disable

Select a user in the middle pane and click **Enable** or **Disable** to enable or disable a selected user's ability to logon to the VSA. This does not affect users already logged onto the VSA. A **Disabled** column in the middle pane indicates whether a user is prevented from logging on to the VSA.

## Log Off

A column in the middle pane indicates whether a user is currently logged on. Select a logged on user,

other than yourself, in the middle pane and click **Log Off** to log off that user. *Users are still logged on if they close their browser without logging off.* The **Minutes of inactivity before a user session expires** setting in System > **Logon Policy** (page 425) determines when the inactive user sessions are automatically logged off.

**Note:** See **VSA Logon Policies** (page 388) for a summary of functions affecting user logons.

## Master User vs. Standard Users

### Master Users vs. Standard Users

A master user is a VSA **user** (page 600) that uses a `Master` user role and a `Master` scope. The `Master` user role provides user access to all functions throughout the VSA. The `Master` scope provides access to all scope data objects throughout the VSA. A `Master` user role can be used with a non-`Master` scope, but a `Master` scope cannot be used with a non-`Master` role. `KServer` management configuration and other **specialized functions** (page 400) can only be performed by `Master` role users. `Master` role users have an additional ability to take ownership of user-defined data objects. The term *standard user* is sometimes used to indicate a user that does not use a `Master` user role and a `Master` scope. When VSA users are listed on a page, a background of two alternating shades of *beige* designates `Master` role users. A background of two alternating shades of *grey* designates non-`Master` role users.

### Master Users

- Any user can be assigned a `Master` user role and `Master` scope, if sufficient roletype licenses exist.
- `Master role` users can view and operate all navigation and control options provided by the user interface.
- `Master scope` users can view, add, edit or delete all scope data objects: organizations, machine groups, machines, departments, and service desks.
- Masters can add or delete any user, including other master users. Since even a master user can't delete their own account while logged on, the system requires at least one master user be defined at all times.

### Standard Users

- A standard role user cannot see roles they have not been granted permission to see.
- A standard scope user cannot see data objects or users they have not been granted permission to see.
- Standard users can create other users, scopes and roles, if given access to these functions.
- A standard user can *not* grant access privileges beyond the ones the standard user has.
- Standard users, if permitted function access, can only create other standard users, not master users.
- By default, a new standard user inherits the scopes and roles of the standard user that created him.
- If a master user creates a new standard user, the standard user inherits *no* scopes or roles. Using this method the master user has to manually assign the scopes and roles of the new standard user.

### Machine Users

- Machine users use machines with VSA agents installed on them. They should not be confused with VSA users who can logon to the VSA.

## System

- Machine users can click the agent icon on the machine's system tray to see a VSA **Portal Access** (page 81) window of functions and data related to that single machine. **Portal Access** is called **Live Connect** (page 380) when accessed from the VSA.
- Access to **Portal Access** functions are determined by the machine role the machine is assigned to. Managed machines are assigned to the `Default` machine role by default and have access to all machine user **Portal Access** functions, unless limited by a VSA user.
- Data object access from the machine is determined by the `Anonymous` **scope** (page 404). Currently, the only data objects enabled by the `Anonymous` scope are **Service Desk** tickets. All other data seen in **Portal Access** is generated by the machine itself.

## Create a New Master User

### Forgotten User Password

If you have forgotten your master user account password, the system provides a way for you to create a new master user account, which enables you to log back in to the system and retrieve the forgotten account information. A master user is a VSA **user** (page 600) that uses a `Master` user role and a `Master` scope.

**Note:** You must have administrator privileges on the KServer. Due to security reasons, you cannot perform the following procedure remotely.

To create a new master user account:

1. Log in to the machine running the KServer.
2. Access the following web page:  
`http://localhost/LocalAuth/setAccount.asp`
3. Enter a new account name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Click **Create**.

You will now be logged in to the system as a new master user.

### Changing the User Password

Change the user password for the original user logon using System > **Users** (page 397).

### If Your Account Is Disabled

If your VSA account is disabled because you entered the wrong password too many times, then you can choose to wait for a set period of time for the account to be automatically re-enabled. By default this time period is 1 hour, but the waiting period may have been adjusted by your VSA system administrator.

If your account has been disabled for another reason, you will have to contact your VSA system administrator to re-enable your account. A disabled user account cannot be re-enabled by resetting the password.

To create a new master account on the KServer see: **Create a New Master User** (page 400).

## User Roles

System > User Security > User Roles

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **User Roles** (page 400) page creates and deletes user roles. Within an user role you can select:

- **Members** (page 401) - Assign or remove members for a user role.

- **Access Rights** (page 401) - Select the access rights for a user role. Access rights determine the functions a user can access.
- **Role Types** (page 402) - Assign or remove role types for a user role. Access rights are restricted by the set of licensed role types assigned that user role.

VSA users can belong to one or more VSA user roles. Each user role must be assigned to at least one user role type.

**Note:** A VSA user logs on with both a user role (functions they can perform) and a scope (scope data objects they can see). Membership in a user role and a scope is independent of each other.

**Note:** VSA users can also be assigned to user roles using the System > Users (page 397) > Roles tab.

**Note:** See System > Users (page 397) for a discussion of the `Master` user role.

**Warning:** Restrict access to **User Roles** and **Roles** for all roles except roles responsible for administrating function access.

## Middle Pane

You can perform the following actions in the middle pane of **Roles**:

- **New** - Create a new role.
- **Copy Permissions** - Copy the access rights to the selected role from any other role.
- **Rename** - Rename the role. Role names can only be all lower case.
- **Delete** - Delete the selected role. All VSA users must be removed from a role before you can delete it.

## Related Pages

The following policies are assigned by user role:

- Access to the entire VSA by weekday and hour using System > **Logon Hours** (page 407)
- Remote control user notification using Remote Control > **User Role Policy** (page 367)
- Field permissions for editing tickets in Ticketing > **Edit Fields** (page 448) and Service Desk > Role Preferences
- **Sharable objects** (page 406)—such as procedures, reports, monitor sets and agent installation packages—can be shared by user role.

## Members tab

The **Members** tab displays which VSA users are assigned to the role selected in the middle pane.

- Click the **Assign** and **Remove** buttons to change the role VSA users are assigned to.
- Sort and filter the VSA users listed in the **Members** page.

## Access Rights tab

The **Access Rights** tab in the System > **User Roles** page determines what functions VSA users belonging to a selected role can perform. For example, access rights can include whether or not a user can open, add, edit or delete a particular record.

**Note:** **Scopes** determine whether a user can see certain user-created data structures displayed in the VSA. **Roles** determine access rights to the functions that act on those data structures.

A navigation tree provides access to each module, folder, item, and control in the VSA.

- Click the  or  icons next to any item in the tree to display or hide child branches of that item.
  - A checked item means a role provides access to that item.

## System

- A unchecked item means a role does *not* have access to that item.
- Click **Expand All** to expand the entire tree.
- Click **Collapse All** to collapse the entire tree.
- Click **Set Role Access Rights** to change access rights for a role.
  - Checking or clearing any checkbox sets the same state for any child items.
  - Click **Enable All** to enable all items.
  - Click **Disable All** to disable all items.

## Specialized Access Rights

- InfoCenter > Dashboard > Admin Notes
- InfoCenter > Dashboard > Status
- InfoCenter > Dashboard > Online Help
- System > System Preferences > Functional Access
- System > System Preferences > Enable Scheduling - Applies to Patch Management > Scan Machine > Schedule button only
- System > System Preferences > Enable Wake on LAN - Applies to Patch Management > Scan Machine > Schedule button only

## Role Types tab

Click the **Assign** and **Remove** buttons to change the role types a user role is assigned to.

## Roles Types

Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the User Roles > **Access Rights** (page 401) tab and Machine Roles > **Access Rights** (page 403) tab. The number of role type licenses purchased displays in the System > **License Manager** (page 420) > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

## User Roles Types

Every user role must be assigned to at least one user role type. If a user role is assigned to more than one role type, access to a function is enabled if any one of the role types enables access to that function. Function access can be optionally limited further by user role or machine role. User role types include:

- **VSA Admin** - Includes both master users and standard users.
- **End Users** - Provides limited access to selected functions in the VSA. Primarily intended for customers of service providers. Customers can logon to the VSA and print reports or look at tickets about their own organizations.
- **Service Desk Technician** - Can edit **Service Desk** tickets and run reports, but not configure service desks, support tables or service desk procedures.
- **Service Desk Admin** - Can do anything in **Service Desk**.

Kaseya **SaaS** (page 599) user role types include:

- **IT Toolkit Free Admin** - Install agents, remote control and file manager with KLC, maintain users and machine groups.
- **IT Toolkit Free Admin** - Install agents, most KLC functions, maintain users and machine groups.
- **IT Workbench Admin** - Basic access to core options with no agent procedures or scripting.
- **IT Center Admin** - Similar to VSA Admin, no system tab access.

## Machine Roles

### System > User Security > Machine Roles

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Machine Roles** (page 400) page creates and deletes machine roles. Machine roles determine what *machine users* see when they use **Portal Access** (page 81)—a version of **Live Connect** (page 380)—from a machine with an agent. The **Portal Access** window displays when a *machine user* double-clicks the *agent icon in the system tray of their managed machine*.

**Note:** The **User Roles** page determines what *VSA users* see when they use **Live Connect** from within the **VSA**.

Within the **Machine Roles** page you can select:

- **Members** (page 403) - Assign or remove machines for a machine role.
- **Access Rights** (page 403) - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- **Role Types** (page 404) - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

**Note:** The Home page seen by machine users when they first display the **Portal Access** window can be customized using System > Customize > **Live Connect** (page 432).

**Note:** See **Enabling Ticketing for Portal Access Users on Unsupported Browsers** (page 82).

**Note:** See the PDF quick start guide, **Live Connect**.

### The Default Machine Role

A predefined **Default** machine role is provided when the **VSA** is installed. Newly created machine ID accounts are automatically assigned to the **Default** machine role when the account is created. If you create other machine roles, you can re-assign machine ID accounts to these other machine roles. You might want to do this if you want to limit machine user access to functions on the **Portal Access** page for different populations of machine users. Each machine ID account can only belong to a single machine role.

### Middle Pane

You can perform the following actions in the middle pane of **Machines Roles**:

- **New** - Create a new machine role.
- **Copy Permissions** - Copy the access rights to the selected machine role from any other machine role.
- **Rename** - Rename the machine role.
- **Delete** - Delete the selected machine role. All machines must be removed from a machine role before you can delete it.

### Members tab

The **Members** tab displays which machines belong to the machine role selected in the middle pane.

- Click the **Change Machine Role** button to change the machine role a machine is assigned to.
- Sort and filter the machines listed in the **Members** page.

### Access Rights tab

The **Access Rights** tab in the System > **Machine Roles** page determines what functions *machine users* can perform on machines belonging to a selected machine role. For example, access rights can include whether or not a machine user has access to their own machine remotely from another machine.

## System

A navigation tree provides access to each item and control on the [Live Connect](#) page.

- Click the  or  icons next to any item in the tree to display or hide child branches of that item.
  - A checked item means a machine role provides access to that item.
  - A unchecked item means a machine role does *not* have access to that item.
  - Click [Expand All](#) to expand the entire tree.
  - Click [Collapse All](#) to collapse the entire tree.
- Click [Set Role Access Rights](#) to change access rights for a machine role.
  - Checking or clearing any checkbox sets the same state for any child items.
  - Click [Enable All](#) to enable all items.
  - Click [Disable All](#) to disable all items.

## Role Type tab

**Note:** In this release of Kaseya 2 there is only one role type, so all machines must use the [Basic Machine](#) role type.

- [Basic Machine](#) - Provides access to all [Portal Access](#) functions available to machine users.

## Role Types

Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the User Roles > [Access Rights](#) (page 401) tab and Machine Roles > [Access Rights](#) (page 403) tab. The number of role type licenses purchased displays in the System > [License Manager](#) (page 420) > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

## Machine Role Types

Every machine role must be assigned to a machine role type. *For the initial release of Kaseya 2, there is only one machine role type.* The machine role type determines the type of *machine-based-license* to apply to machines included in a machine role. For example, if you create a machine role called `StdMach` and assign `StdMach` to the machine role type called `Basic Machine`—and there are 150 machines in the `StdMach` machine role—then the System > [License Manager](#) (page 420) shows 150 of the total number of `Basic Machine` licenses used.

## Scopes

System > User Security > Scopes

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Scopes](#) (page 404) page defines *visibility* of certain types of user-defined data objects throughout the VSA. For example, a user could see some machine groups, but not be able to see other machine groups. Once a scope has made a data object visible to a user, the functions the user can perform on that data object are determined by user role. Scopes enables VSA users responsible for user security to create different scopes of data objects and assign them to different populations of users.

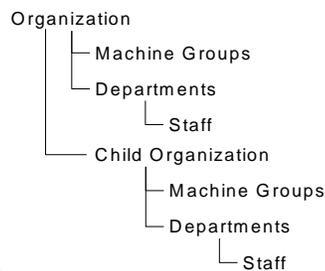
**Note:** A user logs on with both an assigned role (the functions they can perform) and an assigned scope (the data they can see). Membership in a role and membership in a scope are independent of each other.

Users can also be assigned to scopes using the System > [Users](#) (page 397) > Scopes tab.

## Scope Data Objects

For the initial release of Kaseya 2, there are five types of data objects that can be assigned to scopes. Each are defined outside of scopes before being assigned to scopes.

- **Organizations** - Organizations are a new type of record in Kaseya 2. An organization is typically a customer but not necessarily only customers. An organization record contains certain general information, such as its name and address, number of employees and website. An organization also defines a hierarchy of additional information, as illustrated below, representing all the machine groups and personnel within that organization. Organizations are defined using System



> Orgs/Groups/Depts/Staff > **Manage** (page 408).

Machine groups are groups of managed machines. If you've worked with Kaseya 2008, then machine groups behave the same way in Kaseya 2. The only difference is that machine groups are defined by organization. Machine Groups are defined using System > Orgs/Groups/Depts > Manage > Machine Groups.

- **Machines** - A managed machine is a computer with an agent installed on it. Each machine has to belong to a machine group. You create them the same way they are created in Kaseya 2008, typically using the Agents > **Deploy Agents** function.
- **Departments** - Departments are a new type of record in Kaseya 2. A department is a division within an organization. Staff members of an organization are assigned to a department. Departments are defined using System > Orgs/Groups/Depts > Manage > Departments.
- **Service Desk** - A service desk is a new type of record in Kaseya 2. It defines all of the functionality required to process tickets using the new **Service Desk** module. Service Desks are defined using Service Desk > Desk Configuration > Desk Definition.

## Scope Assignment

The parent-child relationships between data structures affect how scopes are maintained.

### Implicit Assignment

Assigning any parent record to a scope *implicitly* assigns all child records to that same scope. For example, assigning an organization to a scope includes the following in that same scope:

- Child organizations.
- Machine groups of the organization and any child organizations.
- Machines of the machine groups in that organization and any child organizations.
- Departments in the organization and any child organizations.

### Explicit Assignment

The only way to include a top level organization in a scope is to manually add it to that scope, because no parent record exists to include it. This is called explicit assignment. You can also explicitly assign a lower level object in scope, *but only if the lower level object is not already assigned implicitly to the scope through its parent*. For example, you could include a machine group explicitly, without adding the machine group's parent organization. You can also explicitly include individual machines and departments in a scope without including their parent records.

### All in Scope

The **Scopes** function provides an **All in Scope** button, when appropriate. The button displays a window that lists all records in a particular Scope tab, regardless of whether records are assigned implicitly or explicitly.

## System

### Master Scope

See System > [Users](#) (page 397) for a discussion of the `Master` scope.

### Middle Panel

You can perform the following actions in the middle pane of [Roles](#):

- [New](#) - Create a new scope.
- [Rename](#) - Rename the scope.
- [Delete](#) - Delete the selected scope. All VSA users must be removed from a scope before you can delete it.

### Scope Details

Each tab provides the following actions:

- [Assign](#) - Assigns access for a data structure to a scope.
- [Remove](#) - Removes access for a data structure from a scope.
- [All in Scope](#) - Displays only on the [Organizations](#), [Machine Groups](#), [Machines](#) and [Departments](#) tabs. Clicking the [All in Scope](#) button on a tab displays a new window listing all data structures of that tab type in the scope, whether defined explicitly or implicitly.

## Sharing User-Owned Objects

Each user has the ability to create user-owned objects—such as filtered views, reports, procedures, or monitor sets. Typically these objects start out as private objects. As a private object no other user can see them or use them. These user-owned objects can be shared with other *user roles* or with individual *users*. In some cases, a `Master` role user can make a user-defined object public for all users. Share options can include the right to use an object, edit, export, delete, or share an object with additional users. Share rights are set by each individual object separately. You can elect to share a user-owned object with:

- Any user roles you are a member of, whether you are currently using that user role or not.
- Any individual users that are members of your current scope.

If share rights for an object are granted by both user role and individual user, share rights are added to one another.

Typically a [Share](#) button displays on any page or dialog that edits a user-owned object. Individual [Share](#) buttons sometimes display next to each user-owned object in a list.

Examples of user-owned objects in the VSA are:

- View Definitions
- Deploy Agent install packages
- Monitoring Dashlets
- Agent Procedures folders
- Service Desk Procedures folders
- Monitor Sets folders
- SNMP Sets folders
- Reports folders
- Report Sets folders
- Service Desk ticket named filters

**Note:** Folder trees have specialized rules about how folders are shared. See [Agent Procedures > Schedule/Create > Folder Rights](#) (page 119) in online user assistance for details.

## Sharing Options

### Kaseya 2 Share Options

- Adding a user or user role to the **Shared Pane** allows that user to use that object. No additional rights, including **View**, have to be assigned to the user or user role to use that object.
- Checking any *additional rights*—such as **View**, **Edit**, **Create**, **Delete**, **Rename**, or **Share**—when you *add* the user or user role, provides that user or user role with those additional rights. You have to remove the user or user role and re-add them to make changes to their additional rights.
- **View** does not refer to being able to view the object. **View** means the object's configuration can be viewed but not edited. If an export option is provided, **View** also enables the user to export the object.
- **Share** means the users or user roles can assign share rights.

### Legacy Share Options

Certain functions in Kaseya 2 still set sharing rights using a legacy dialog as follows:

- Share rights are assigned *by object*. There are three sharing checkbox options. The first two checkboxes are *mutually exclusive* and determine what share rights are assigned. If neither of the first two checkboxes are checked, the shared object can only be seen by the users given share access, but the object cannot be used nor edited. The **Shared** and **Not Shared** list boxes and the third checkbox determine who can see the object.
  - **Allow other administrators to modify** - If checked, share rights to the object includes being able to use it, view its details and edit it.
  - **Other administrators may use but may not view or edit** - If checked, share rights to the object only allows using it.
- **Make public (seen by all administrators)** - If checked, ensures that *all* current and future VSA users can see the object. If blank, only selected user roles and users can see the shared object. If blank, and new users or user roles are added later, you have to return to this dialog to enable them to see the specific object.

## Taking Ownership

When you first create a user-owned object, you are the owner of that object. A user-owned object can only be *owned* by one user at a time. The owner of an object always has "full rights" to that object.

Master role users have an additional right, called **Take Ownership**, that allows them to take ownership of any user-*shared* object. When a user-shared object is selected or edited by a master role user, a **Take Ownership** option displays. When ownership is taken, the new owner of that object now has "full rights" to the object.

Typically the reason you take ownership of a shared object is to maintain its contents because the original owner can't do so. For example, the owner of a shared object may have left the company and no longer be available. In most cases, master role users can work within the share rights they've been assigned by other VSA users.

**Note:** Deleting a VSA user from the system assigns ownership of all objects belonging to that VSA user to the VSA user performing the delete.

**Note:** A master role user can check the **Show shared and private folder contents from all users in System > Preferences** (page 391) to see all shared and private folders. For Private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

## Logon Hours

### System > Logon Hours

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

## System

The [Logon Hours](#) page determines *when* users can logon to the VSA by specifying the weekdays and hours for each user role. Each day of the week can have different hours of operation set.

**Note:** See [VSA Logon Policies](#) (page 388) for a summary of functions affecting user logons.

### Select user role

Select a [user role](#) (page 367) to display and maintain its logon hour settings.

### No Hours Restrictions

If checked, users can logon to the VSA at any time and day of the week. Uncheck to enable all other settings.

### Deny

Denies logon access for the entire weekday.

### or allow between <12:00 am> and <12:00 am>

Specify the range of time logons are allowed. All times are in the KServer's time zone. For all day access, set start and end time to the same time.

## User History

### System > User History

- This page applies to the following products: [On Premises](#), [Kaseya Advanced](#), [Kaseya Essentials](#), [IT Center](#), [IT Workbench](#)

The [User History](#) page displays a history, in date order, of every function used by a user. The history also displays any actions captured by the [System Log](#) (page 423) performed by the selected user. The system saves history data for each user for the number of days specified for the [System Log](#).

Click [a user name](#) to display the log for that user.

**Note:** This log data does not appear in any reports.

---

## Orgs/Groups/Depts/Staff

- [Manage](#) (page 408) - Create organizations, machine groups, departments and staff.
- [Set-up Types](#) (page 411) - Create organization types used to classify organizations.

## Manage

### System > Orgs/Groups/Depts/Staff > Manage

- This page applies to the following products: [On Premises](#), [Kaseya Advanced](#), [Kaseya Essentials](#), [IT Center](#)

The [Manage](#) page defines the organizations you do business with. Typically an organization is a customer, but an organization could also be a business partner. Organizations are associated with [Scopes](#) (page 404), tickets and with desk definitions.

Within an organization you can define:

- [General](#) (page 409) - General settings for the organization.
- [Machine Groups](#) (page 410) - Machine groups associated with this organization.
- [Departments](#) (page 410) - A unit of administrative responsibility within an organization.
- [Staff](#) (page 410) - Personnel assigned to a department.

- **Custom Fields** (page 411) - Assigns values to custom fields used to classify organizations.

## Manage > General tab

Click **New** to display the **Add Organization** window, or click a row in the middle panel, then click **Edit** to display the **Change Organization** window. Enter the following attributes:

- **New/Convert** - Select **New Organization** if no other data source exists to convert from. If **Service Billing** is installed you can create a organization by **converting** (page 594) an existing customer record or vendor record.
- **ID** - The record identifier. Can only be changed using the **Rename** button.
- **Org Name** - The display name for the identifier.
- **Org Type** - The type of organization. See **Organization Types** (page 411).
- **Default Dept. Name** - The default department for the organization.
- **Default MachGroup Name** - The default machine group for the organization.
- **Org Web Site** - The organization's web site.
- **Number of Employees** - The number of employees in the organization.
- **Annual Revenue** - The annual revenue of the organization.
- **Preferred Method of Contact** - The organization's preferred method of contact: Phone, Email, Mail, Fax.
- **Parent Organization** - The parent organization of this organization. The parent organization must be previously defined to display in this drop-down list.
- **Primary Phone** - The primary phone of the organization.
- **Primary Email** - The primary email of the organization.
- **Primary Contact** - The primary contact for the organization. A contact is a **staff** (page 410) member of a department.
- The address of the organization:
  - **Country**
  - **Street**
  - **City**
  - **US State**
  - **Zip Code**
- **Map** - Clicking this hyperlink displays the location of the address in Google maps.

### Pre-Defined Organizations

Three pre-defined organizations are provided:

- **myOrg** is the **organization** (page 594) of the service provider using the VSA. All other organizations in the VSA are second party organizations doing business with **myOrg**. The default name of **myOrg**, called **My Organization**, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the myOrg organization.*
- **Kserver** is the org assigned to agents installed on your KServers. This makes it easy to apply specialized settings to KServers, which are typically maintained differently from other agent managed machines.
- **Unnamed** is the default organization to assign an agent. Maintaining multiple agent install packages in Agent > **Deploy Agents** (page 39), one for each organization, can be time consuming. Instead some server providers use a single agent package for the **unnamed** organization and perform all installs using this package. System > **Naming Policy** (page 395) can reassign new agents to the correct organization.group ID automatically—the first time the agents check in—based on each managed machine's IP or connection gateway. Agent > **Copy Settings** (page 70) may be used

## System

afterwards, to manually copy specific kinds of agent settings by [machine ID template](#) (page 592) to the type of machine revealed by the initial audit.

## Manage > Machine Groups tab

Define the machine groups associated with this organization. Machines are always defined by machine group and machine groups are always defined by organization. You can define multi-level hierarchies of machine groups by identifying a parent machine group for a machine group when the machine group is created.

### Adding / Editing a Machine Group

For a new machine group enter the following attributes:

- **Name** - The name of the machine group.
- **Parent Group** - Parent machine group. Optional.

## Manage > Departments tab

Departments can be defined within an organization, customer record or vendor record. Example: *IT, Sales or Accounting*. All staff members are defined by the department they belong to. You can define multi-level hierarchies of departments by identifying a parent department for a department when the department is created. You can reassign a staff member to any other department within the same organization, customer record, or vendor record.

### Adding / Editing a Department

For a new department enter the following attributes:

- **Name** - The name of the department.
- **Manager Name** - The name of the department manager. Optional. You must create a staff member before you can assign that staff member as the manager of the department.

## Manage > Staff tab

Create staff members within departments and maintain contact information for each staff member. Contacts and their phone numbers can be associated with tickets and with desk definitions. Staff member information can also be updated by Active Directory using Agent > [View AD Users](#) (page 66).

### Adding / Editing a Staff Record

- **Full Name** - The full name of a person within the organization.
- **Department** - The department the person is associated with. The department must be previously defined to display in this drop-down list.
- **Supervisor** - The person this staff member reports to. The Supervisor must be previously defined as a staff member in the same department.
- **Title** - The person's title in the organization.
- **Function** - The function the person performs in the organization.
- **Phone Number** - The person's direct phone number.
- **Email Address** - The person's email address.
- **User Name** - VSA user ID associated with this staff member. Required to [View All Tickets](#) and for [Time Tracking](#) (page 453).
- **View All Tickets** - If checked, the VSA user associated with this staff member can view all tickets in his or her scope as well as tickets associated with this specific staff member record. If blank, this VSA user can only view tickets associated with this specific staff member record.

*Time Approval*

A staff member record must be associated with a VSA user to approve timesheets and have visibility of **timers** (page 461).

- **Approve All Timesheets** - If checked, this staff member can approve any timesheet in his or her partition. This ensures all timesheets can be approved in a timely manner, if other approvers are temporarily unavailable.
- **Approval Pattern** - Specifies the approval pattern required to approve this staff member's timesheets. Approval patterns determine whether the staff member's supervisor, or the supervisor's supervisor, or both, are required to approve the staff member's timesheet.

**Note:** See **Time Tracking** (page 453) configuration options.

### Visibility of Service Desk Tickets by a Staff Member

If a VSA user name is associated with the staff member record of an organization, then that VSA user has visibility of tickets associated with that staff member record *even if the VSA user's scope does not allow it*. Any tickets created by that VSA user are automatically associated with their staff member record and organization. This method primarily supports machine users using **Portal Access** (page 81) to create and manage their own tickets. Machine users expect to have access to all the tickets they create and to any tickets created on their behalf, but may have no scope privileges defined for them. If a scope does exist for a VSA user associated with a staff member, checking the checkbox called **View all tickets** in the **staff member** (page 410) record provides visibility of those additional tickets by scope.

**Example:** Dale is the main customer contact for the XYZ organization. He is provided a scope that allows him to see all tickets related to his organization, even tickets not created by him, so the **View all tickets** checkbox is enabled. Brandon from the XYZ organization contacts the service desk to submit a ticket as well. Initially it's unclear whether Brandon should have access to any other tickets beyond the tickets he himself creates, so the **View all tickets** is left unchecked. Later, if Dale okays greater access for Brandon, the service desk provider can assign a scope to Brandon and check the **View all tickets** checkbox.

## Manage > Custom Fields tab

Assign values to the custom fields displayed on this tab. The values you assign are used to classify organizations. The titles of the custom fields displayed on this tab can be customized using Site Customization > **Org Custom Field Title** (page 430).

## Set-up Types

System > Orgs/Groups/Depts > Set-up Types

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Set-up Types** page defines records that classify your organizations. For example, you might define an organization as a `division` within your enterprise, or classify organizations regionally or by revenue. Alternatively, you might classify organizations as a `prospect`, `preferred customer`, or `business partner`. It depends on your business requirements.

### Service Desk

**Set-up Types** can be optionally used to automatically associate a ticket with a policy in the **Service Desk** module.

### General tab

Click **New** to display the **Add Organization Types** window, or click a row in the *middle* panel, then click **Edit** to display the **Change Organization Types** window. Enter the following attributes:

- **ID** - The record identifier. Can't be changed once you save it.
- **Description** - A brief description of this ID.

---

## Server Management

### Request Support

#### System > Request Support

- This page applies to the following product: On Premises

The **Request Support** page provides multiple ways of contacting Kaseya support.

**Note:** Please reference our additional documentation before calling support.

- **Support Web Site** - Find answers to common questions using the Kaseya Support website at <http://www.kaseya.com/support.aspx> (<http://www.kaseya.com/support.aspx>). This website provides links to the **Kaseya Support Forum** and to the **Kaseya Support Knowledge Base**. The Support Forum hosts an interactive community of Kaseya users that discuss a wide variety of issues and solutions on a daily basis. Subscribe to the forum to get new posts of interest directly emailed to you as new information appears. The Kaseya Knowledge Base provides technical information about installation and usage of the Kaseya IT Automation Framework.
- **Enable Kaseya Support to Logon** - Kaseya support engineers can solve problems with your system quickly and efficiently when they can directly access your KServer. Click **Create** to create a `kaseyasupport` master user account on your system. The Kaseya Support engineer can use our system to log into your system and help solve any problems.

**Note:** We realize the security implications of providing access to your KServer. To protect this logon, your system creates a secure logon. No one has access to the password, not even the Kaseya support engineer. The password gets changed every time you click this button.

- **Kaseya Portal** - The **Kaseya Portal** (<https://portal.kaseya.net>) provides a single point of contact for managing your Kaseya account. You can create and view support tickets with Kaseya, receive training, view announcements of upcoming events and acquire other services. You can also link to the user forum and and knowledge base from this site.

### Your Information

Typically Kaseya support needs some basic information about your system to begin providing support. Your user name, email address, Customer ID, and system URL are provided for your convenience.

## Configure

#### System > Configure

- This page applies to the following product: On Premises

The **Configure** page manages the configuration of your KServer and related services.

**Note:** For the latest instructions on migrating an existing KServer to a new machine see [Moving the Kserver section in the the KB article latest Kserver installation and upgrade user guide](http://help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp) ([help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp](http://help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp)).

### Check for Update

Click **Check for Update** to determine if your KServer is the latest version available. If an update exists, a message alerts the master role user that an update is currently available and is applied at the next

master role user logon. An update is only downloaded if the version currently running is older than the version available. Otherwise, no action is performed.

## Version Number

Shows the version number of the system software and the **hotfix** (page 590) level of your system.

## Warn if the server cannot get updates from <http://vsaupdate.kaseya.net>

Check this box to display a warning if your VSA cannot connect to <http://vsaupdate.kaseya.net> to fetch the latest hotfix checker list, the latest PCI ID list used by audit, or the VSA software update notifications. Your VSA attempts to automatically fetch this information from <http://vsaupdate.kaseya.net> on port 5721. Verify that **port 5721 outbound** is not blocked by your firewall.

## Warn when the license reaches the maximum number of seats

Check this box to display a warning when the number of machine ID accounts reaches the maximum for your VSA.

## Hotfixes

Several options affect how **hotfixes** (page 590) update your KServer.

**Note:** You can reference the latest hotfix level in [System > License Manager](#) (page 420).

- **Enable automatic check every day at <TIME>** - If checked, your KServer checks <http://vsaupdate.kaseya.net> for *new only* hotfixes each day at the specified time of day. If any new hotfixes are available, the KServer automatically downloads and applies the hotfixes without any user interaction.
  - **Reload** - Displayed if **Enable automatic check** is checked. Click to reload *all hotfixes since the base release* of the version of KServer your system is running.
  - **Process Hotfix** - Displayed if **Enable automatic check** is blank. Click to install a previously tested list of hotfixes. Typically these hotfixes were installed and tested on a staging KServer and are approved for installing on a production KServer. See **Processing Hotfixes Manually** (page 417).
- **Get Latest Hotfix** - Click to check if new hotfixes are available *immediately* and, if they are, download and apply them.
- **Manually apply hotfixes** - If your system is not connected to the internet or can not reach <http://vsaupdate.kaseya.net>, then click this link.
  - **Check Now** - Click to force the system to check for new hotfixes *immediately*. If any new hotfixes are available, they are downloaded and automatically applied. Only *new* hotfixes get loaded.
  - **Reload** - Click to re-download and apply all hotfixes for the version of KServer your system is running.
- **Pending Hotfixes** - Click to display a list of hotfixes that are available to apply.
- **Hotfix History** - Click to display a history of applied hotfixes.

## Database

- Click **Reapply Schema** to re-install and validate the last database schema that was downloaded using **Check for Update**. Reapply schema is a safe operation that users can run in an attempt to resolve a variety of problems. Reapply schema:
  - Sets default values and runs basic consistency checks on the database.
  - Rebuilds all pre-defined Kaseya procedures.
  - Rebuilds all pre-defined Kaseya procedure samples.

## System

- Reschedules default backend processing procedures for the KServer.

This is all completed without the risk of losing any agent data. This is a good self healing routine to run if you observe:

- Procedures failing in the **IF** condition or in specific steps.
- Pending alerts not being processed within a two minute interval. You can monitor this using the System > **Statistics** (page 423) page. This might indicate a problem with backend processing procedures.
- Click **Defrag Database** to defragment the physical files on your disk arrays. Fragmented SQL Server data files can slow I/O access.

**Warning:** Do not use the Microsoft SQL tuning advisor against the schema. It adds keys that conflict with the smooth operation of the system.

## Sample Data

- **Reload sample scripts with every update and database maintenance cycle** - Check to reload sample agent procedures.
- **Reload sample event sets with every update and database maintenance cycle** - Check to reload sample event sets.
- **Reload sample monitor sets with every update and database maintenance cycle** - Check to reload sample monitor sets.

## HTTPS

- **Automatically redirect to https at logon page (except when accessing via localhost)** - If checked, ensures all users logging into the VSA remotely use the secure HTTPS protocol.

## API

- **Enable VSA API Web Service** - Check to enable the **VSA API Web Service** (page 513).

## Invalid Patch Location Notification

- **Enable Invalid Patch Location Notifications** - Microsoft sometimes prepares patches that do not allow the **File Source** (page 340) function to download patches successfully. If checked, this option notifies Kaseya that an "invalid patch location" exists for a patch required by any of the managed machines on your system. Notification alerts Kaseya to prepare a valid patch location manually and send it out as an updated patch location override for all customers to use. If blank, no notification is sent to Kaseya. You will still receive updated patch location overrides prepared in response to notifications reported by *other* customers, regardless of this setting.

**Note:** Notification sends no customer-specific or machine-specific information to Kaseya.

## Downloading Attachments in Ticket Notifications

- **Allow non-authenticated users to download attachments from ticket notifications** - If checked, links to attachments embedded in the notes of tickets can be opened in outbound emails without requiring the user to authentic themselves to the VSA. For security reasons, enabling this option is not recommended.

## Backups

- **Run database backup / maintenance every <N> Days @ <Time>** - The KServer automatically backs up and maintains the MS-SQL database and transaction log for you. Click **Set Period** to set the frequency and time selected. If your KServer is shut down at the scheduled backup time, the backup will occur the next time the KServer goes online. You can enter zero to disable recurring backups.

- **Backup folder on KServer** - Set the directory path to store database backups in. The default directory path is typically `C:\Kaseya\UserProfiles\@dbBackup`. Click **Change** to confirm changes to the directory path. Click **Default** to reset the directory path to its default.

**Note:** Database backups older than three times the backup and maintenance period are discarded automatically to prevent your disk drive from filling up. For example, if the backup occurs every 7 days, any backup older than 21 days is deleted.

- **Change DB** - Connect your KServer to a database on a different machine.
  1. Backup your existing `ksubscribers` database by clicking **Backup Now**.
  2. Copy the database backup file to the database server you wish to connect to.
  3. Verify your new database is set to **mixed mode authentication**.
    - ✓ Open the **SQL Enterprise Manager**.
    - ✓ Right click the database and select properties.
    - ✓ Click the **Security** tab.
    - ✓ Under authentication, select **SQL Server and Windows**.
    - ✓ Click **OK**.
  4. Verify CLR is enabled in the new database server.
  5. Verify your KServer is on the same LAN as your new database server and **port 1433** is open on the database server.
  6. Click the **Change DB** button.
  7. Enter the database location using one of the following formats:
    - ✓ computer name
    - ✓ computer name\instance name
    - ✓ IP address
  8. Enter a database logon name. The default logon name is `sa`.

**Note:** This logon is only used to configure the database. The system creates its own database logon to use going forward.

9. Enter the password associated with this logon name.
  10. Click **Apply**. The system then connects to the remote database and configures it.
  11. Click **Restore** to load the data from the back up file you made in step one into your new database.
- **Backup Now** - Initiate a full database backup now. Use this function *before* you shut down or move your KServer, to ensure you have the latest KServer data saved to a backup. The backup will be scheduled to run within the next 2 minutes.
  - **Restore** - Click to restore the KServer's database from a backup file. A file browser displays a list of KServer database backup files you can restore from.

**Note:** After a restore of a 5.1 database, the SSRS URL will be invalid and need to be reset. After a restore of a 6.x database the SSRS URL may be invalid and need to be reset.

## Archive

Archiving of agent logs are enabled, by log and machine ID, using Agent > **Log History** (page 35).

- **Archive and purge logs every day at <time>** - Specifies the time of day log files are archived and purged.
- **Set Period** - Click to confirm changing the time log files are purged and archived.
- **Log file archive path** - The file location where the archive files are stored.

**Note:** Monitoring data log archives are stored in the <KaseyaRoot>\UserProfiles\@dbBackup directory. This is to improve performance on systems where the database is on a different server. All other agent log archives are stored in the directory specified by the System > Configure (page 412) > Log file archive path field.

- **Change** - Click to the confirm changing the archive file location. A procedure runs to move any existing archive files in the old file location to the new file location.
- **Default** - Resets the log file archive path to the default location on the KServer. A procedure runs to move any existing archive files in the old file location to the new file location.

### Service Status

- **KServer Log** - Displays the last 300 kbytes of the KServer's log file. The entire log file is up to 5 Mbytes in size and is located at xx\KServer\KServer.log where xx is the parent directory of the VSA web directory.
- **Live Connect KServer** - An agent is automatically installed on the Kserver. You can click the check-in icon for this agent to initiate a **Live Connect** (page 380) session with the Kserver.
- **Stop KServer** - Shows the current status of the KServer: **running** or **stopped**. The KServer can be stopped by clicking **Stop Service**.
- Clear the **Enable alarm generation** box to prevent generating unnecessary alarms. This can occur if you stop the KServer, disconnect from the internet, or maintain the system. Otherwise leave this box checked.
- **Restart MsgSys** - Restarts the MessageSys service. This service is the application server that manages requests from VSA application users.
- **Enable logging of procedure errors marked "Continue procedure if step fail"** - If checked, failed steps in procedures are logged. If blank, failed steps in procedures are *not* logged.
- **Restart Network Discovery** - Restarts the Network Discovery service if the service has stopped.

### Select time format

Click the appropriate radio button to select how time data is displayed. The default is AM/PM format. Both these display formats are compatible with Microsoft Excel.

- AM/PM format - 9:55:50 pm 9-Apr-07
- 24-hour format - 21:55:50 9-Apr-07

**Note:** Time offset is set in System > Preferences (page 391).

### Change external name / IP address of Server

Shows the current external name or IP address of the KServer. This is the address the agents of managed machines access for check-in purposes. The address can be changed by entering a new address or host name in the field and pressing **Change Name/IP**.

**Note:** Do *not* use a computer name for your KServer. The agent uses standard WinSock calls to resolve a IP address from a fully qualified host name. Resolving an IP address from a computer name requires NETBIOS, which may or may not be enabled on each computer. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

### Set URL to MS-SQL Reporting Services Engine

Click the **Change URL...** (page 418) button to specify the URL used by the VSA to connect to Reporting Services. You can also specify the credential used to access Reporting Services and customize the URL displayed in the header of all VSA reports.

## Change System Server Port

Specify port **Agents check into Server with** - Entering a different port and clicking **Change Port** switches the port the KServer uses *immediately*.

**Warning:** Before you change the KServer port ensure that all agents are set to use the new port with their primary or secondary KServer. Agent check-ins are configured using *Agent > Check-in Control* (page 75).

## KServer ID

ID used to bind agents to the Kserver - The unique identifier for this Kserver. Bound agents cannot check-in successfully unless the unique Kserver ID they are bound to using the Agent > **Check-in Control** (page 75) page matches the unique ID assigned to the KServer using the System > **Configure** (page 412) page. Only change the KServer ID if you are installing a fresh VSA and wish to duplicate the ID of an existing KServer with agents already bound to it.

## Version Information

Displays the following information about your VSA configuration.

- OS Version
- IIS Version
- KServer Version
- SQL Version
- Database Location
- Agent On KServer

## Release Notes

Click **Release Notes** to display a list of all changes and enhancements made to the VSA, for all versions of the software.

## Show License

Click **Show License** to display the current license agreement to use the VSA.

## Processing Hotfixes Manually

You can install and test hotfixes on a *staging* KServer, then copy the list of tested hotfixes to your *production* KServer using the following procedure.

**Note:** All steps refer to the System > **Configure** (page 412) page, unless a specific step says otherwise.

1. Disable the **Enable automatic check** checkbox on the *production* KServer.
  - **Do not click** the **Process Hotfix** button on the *production* KServer until instructed to so at the end of this procedure.
  - **Do not click** the **Get Latest Hotfix** button **ever** on the *production* KServer.
  - **Do not click** the **manually apply hotfixes** link **ever** and install hotfixes that way.
2. Create a copy of the *production* KServer and call it the *staging* KServer.
3. Check the **Enable automatic check** checkbox on the *staging* KServer.
4. Click the **Reload** button on the *staging* KServer. This ensures all hotfixes are reloaded from the base release up to the latest hotfix.
5. Uncheck the **Enable automatic check** checkbox on the *staging* KServer. This ensures no more hotfixes will be added to your *staging* KServer during your cycle of testing.

## System

6. Make a note of the hotfix level of your *staging* KServer and all add-on modules using System > **License Manager** (page 420).
7. Test your critical business processes on the *staging* KServer.
  - **Report any problems** (<mailto:support@kaseya.com>) with the latest batch of hotfixes on your *staging* KServer, if necessary. Additional hotfixes may be required to correct any problems you encounter.
  - Repeat steps 3 through 7 on your *staging* KServer until you are satisfied the latest hotfix level is acceptable for use on your *production* KServer.
8. Locate the `kweb*` files on the *staging* KServer. Typically these files are located at: `C:\Kaseya\WebPages\install`. There is a single file for the VSA and one additional file for every installed add-on module.
  - `kweb.xml` - The VSA hotfix file.
  - `kweb-sd.xml` - The Service Desk hotfix file.
  - `kweb-kes.xml` - The Endpoint Security hotfix file.
  - `kweb-budr.xml` - The Backup hotfix file.
  - `kweb-kusm.xml` - The Desktop Policy and Migration hotfix file.

**Warning:** Do not modify these `kweb*` files manually. All hotfixes in the `kweb*` files must be installed in sequence as specified by Kaseya.
9. Copy and paste these `kweb*` files from the *staging* KServer to the same relative location on the *production* KServer.
10. Click the **Process Hotfix** button on the *production* KServer. The tested `kweb*` hotfixes are now installed on the *production* KServer.
11. Confirm the hotfix levels of your *production* KServer and all add-on modules match the hotfix levels on your *staging* KServer using System > **License Manager** (page 420).

## Set URL to MS-SQL Reporting Services Engine

System > Configure (page 412) > Change URL...

The **URL to MS-SQL Reporting Services** dialog configures the VSA connection to the SQL Services Reporting Services (SSRS) instance used to generate VSA reports. The SSRS may be installed locally or remotely from the KServer and locally or remotely from the SQL Server instance hosting the `ksubscribers` database.

**Note:** Installing or updating the VSA to Kaseya 2 allows you to bypass configuring the SSRS until after the installation or update.

Settings include:

- **Host Name** - The URL used by the VSA to connect to a SQL Server Reporting Services instance. Mandatory to run reports.
- **Logo** - The URL of the image displayed in the header of reports. Applies to some configurations.
- **User Name** - The user name used to access the Reporting Services instance when running reports. Applies to some configurations.

**Note:** - See the Kaseya SSRS Configuration user guide for a visual walkthrough of the steps described in this topic.

### Host Name

The VSA typically uses one of the following URL patterns to connect to a SQL Server Reporting Services instance. Specifying the appropriate URL is mandatory to run reports.

## SQL on the same box as VSA

```

http://localhost/ReportServer (most common)
http://localhost/ReportServer$SQLEXPRESS
http://localhost/ReportServer$<SQLINSTANCENAME> (2005)
http://localhost/ReportServer_<SQLINSTANCENAME> (2008)
http://localhost:<PORTNUMBER>/ReportServer$<SQLINSTANCENAME> (2005)
http://localhost:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME> (2008)

```

## SQL box separate from VSA

```

http(s)://<SQLSERVERNAME>/ReportServer (most common)
http(s)://<SQLSERVERNAME>/ReportServer$SQLEXPRESS
http(s)://<SQLSERVERNAME>/ReportServer$<SQLINSTANCENAME> (2005)
http(s)://<SQLSERVERNAME>/ReportServer_<SQLINSTANCENAME> (2008)
http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer$<SQLINSTANCENAME> (2005)
http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME> (2008)

```

## Logo

By default, VSA report headers display the image specified by the System > Site Customization > **Site Header** (page 429). Changing the value in the System > Configure > **Change URL...** (page 418) > **Logo** field overrides this default, changing the URL *for report headers only*. Changing the URL in the Change URL... > **Logo** field does not affect the display of the Site Header image.

If a logo does not display in SSRS reports it may be due to either of the following conditions:

- The SSRS is installed on the same machine as the KServer. SSRS is unable to retrieve the logo because of firewall issues. Change the URL to `localhost` from the externally available URL/IP address.
- The VSA has been configured using a self-signed SSL certificate. Change the protocol from `https` to `http`.

## User Name

You can provide all VSA users with a credential that lets them run SSRS reports. This eliminates the need to maintain access rights for each VSA user requiring access to the SSRS. This applies in particular to VSA users in a workgroup instead of a domain, who don't have a centralized method of authentication such as Active Directory to manage access rights to the SSRS.

Credentials are specified in three locations:

- User Accounts in the system hosting the SSRS.
- SSRS Report Manager.
- VSA > System > Configure > Change URL... > User Name

This procedure creates a dedicated user—in this example, `KaseyaReport`—in the system hosting the SSRS. The SSRS **Report Manager** is used to give the `KaseyaReport` user access to running reports in the SSRS. Finally, the `KaseyaReport` credential is registered in the System > Configure > Change URL... > User Name fields. From that point forward the VSA uses that credential to access the SSRS every time a VSA user runs a report.

1. On the system hosting the SSRS, add a `KaseyaReport` user using the **Microsoft Management Console**. Using the console enables you to set the checkboxes below for the new user.
  - Give the user a strong password.
  - Uncheck the **User must change password at next logon** field.
  - Check the **User cannot change password** and **Password never expires** fields.
2. Apply appropriate permissions to the new user for your environment.
3. On the system hosting the SSRS, open a browser and type in the URL for **Report Manager**, for example, `http://localhost/Reports`, using the **Administrator** account.
4. Click **Site Settings** at the top right hand corner.
5. Click **Security** in the left hand sidebar.
6. Click **New Role Assignment** along the menu bar.

## System

7. Enter the username that was created in step 1 in the **Group or user name** field, for example, `KaseyaReport`.
8. Select **System User** checkbox.
9. Click **Add**.
10. In the VSA, display the System > Server Management > **Configure** page. Click on the **Change URL** button to open the dialog.
11. Click on the **Edit** button at the top of the page.
12. Enter the credential you defined in step 1 and make sure the **Specify Account** checkbox is checked. This means SSRS will use the credential you entered. If the user, for example `KaseyaReport`, is not a domain user you can leave the **Domain** field blank.
13. Click **Save** and then click on the **Test** button to test the changes.

## License Manager

### System > License Manager

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **License Manager** page allocates machine licenses by org ID or group ID. This page also displays the number of user licenses purchased for each role type. If necessary, you can kill user sessions from the page to enable other users to logon.

Types of licenses managed include:

- Agent licenses - applies to machines by organization, group or group ID
- Role type licenses - applies to VSA users or machines by role type

Add-on module licenses only display if you have purchased and installed those add-on modules.

### Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a **machine ID template** (page 592). Machine ID template accounts are not counted as "used" until you install the agent.

## General tab

The **General** tab displays the products you have purchased.

### Update Code...

Click the **Update Code...** to enter a new license code or reapply your existing license code.

### Show License

Click **Show License** to display the current license agreement to use the VSA.

### (Header Information)

Displays the following information about your VSA configuration.

- **Kaseya Managed Services Edition** - The version number of the KServer.
- **License Code** - The current license code for this KServer.
- **Expiration Date** - The current expiration date for running the system "as is" with the current license code.
- **Maintenance Expiration Date** - The current expiration date of maintenance services, including upgrades, hotfixes and access to tech support.
- **Latest Hotfix Level** - The latest hotfix level for the VSA.

### Product Name Table

Displays the following information about your add-on modules.

- **Product Name** - The version number of the KServer.
- **Version** - The version number of the product.
- **Status** - The status of the product: *Installed*.
- **Latest Hotfix Level** - The latest hotfix level for the add-on module.
- **Usage Type** - The level of functionality enabled for the product. Applies across all role types. See Service Desk Licensing.

## Licenses tab

The **Licenses** tab displays the number of agent-based licenses for each product you have purchased. You can allocate portions of the total number of agent licenses you have purchased for a product to specific organization and machine groups.

### (License Type Table)

The license type table displays the following:

- **License Type** - Lists each product you have purchased that requires an agent-based license. This can include:
  - Agents - VSA agents
  - KBU - Workstation clients
  - KBU - Servers clients
  - KES - Endpoint Security clients.
  - KDPM - Desktop Policy and Migration clients.
- **Used** - The current number of managed machines that have this product installed.
- **Max** - The maximum number of managed machines that can install this product

### Change License Allocations

The total number of licenses available can be allocated to a specific organization, group or sub-group ID. Select any organization, group or sub-group in the allocation table, then click the **Change License Allocations** button.

### (Allocation Table)

The allocation table displays the following:

- **Organization/Machine Group** - Lists both organizations and groups within organization in a single column. You select any row to allocate agent licenses to that row.
- **Type** - *Org* or *Group*. Machine groups can include machine sub-groups.
- **Agents Used** - The current number of managed machines that have this product installed in this organization or machine group.

## System

- **Agents Max** - The maximum number of managed machines that can install this product in this organization or machine group.

## Role Types tab

The **Role Types** tab displays the license counts you've purchased for each role type in your VSA. Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the User Roles > **Access Rights** (page 401) tab and Machine Roles > **Access Rights** (page 403) tab. The number of role type licenses purchased displays in the System > **License Manager** (page 420) > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

- **RoleType** - The name of the roletype.
- **Description** - The description of the roletype.
- **Max Named Licenses** - The maximum number of users licensed for this roletype.
- **Max Concurrent Licenses** - The maximum number of current users licensed for this roletype.

## View Sessions

Click a role type, then click **View Sessions** to display a list of current VSA user sessions using that role type. You can select one or more sessions and click **Log Off Selected Sessions** to end those sessions. Use this feature to log off unnecessary sessions if a user is unable to logon because a roletype maximum of *concurrent* sessions has been reached.

## Import Center

### System > Import Center

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Import Center** page imports and exports automation solutions—user-defined data structures that can be applied to multiple agents—into and out of the VSA. This enables you to migrate automation solutions between VSAs, or import automation solutions from other solution providers. These include:

- Packages
- Agent Procedures
- Agent Templates
- Event Sets
- Holiday
- Monitor Sets
- Monitor SNMP Sets
- Patch Policies
- Sample Exportable Items
- Views

You can import or export multiple items of multiple types using a single XML. For example, you may want to import a set of agent procedures and monitor sets that are both used together for form a single automation solution.

## Imports tab

Use this tab to import an automation solution XML into your VSA.

- **New Import** - Select an XML file to import, then click the **Process** button.
- **View Import Details** - Displays a history of the import.

The paging displays a log of the files you have imported.

## Exports tab

Use this tab to export an automation solution XML into your VSA.

- **New Export**
  1. Select the type of automation solution to export.
  2. Select one or more items of that type to export.
  3. **Click the Continue button to add another type of automation solution.**
  4. Click the **Export** button to export. A single XML file is created that is still stored on the Kserver.
  5. Click the hyperlink for the newly exported file that displays in the table grid of the Exports page.
  6. Confirm saving the file to your local machine.
- **View Import Details** - Displays a history of the export.

## System Log

### System > System Log

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **System Log** page logs events that cannot be tracked by machine ID, for a specified time period. *This log captures events not contained in any of the agent logs.* Examples include:

- Deleting machine IDs
- Failed and successful logon attempts
- Video streaming sessions
- Starting/stopping of the KServer
- Deleting trouble tickets assigned to a group (not a machine)
- Scheduling reports

### Save History to N Days

Click **Apply** to save system log events for the specified number of days.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

### Search

The search function acts as a filter on the **Description** field. Enter a set of words to search for and click the **Search** button. Only rows matching the search criteria are listed. Use % or \* as a wild card. Use the underscore character (\_) as a single character placeholder. Text is case insensitive.

**Note:** This log data does not appear in any reports.

## Statistics

### System > Statistics

- This page applies to the following product: On Premises
- Related information is provided using Reports > Network Statistics (page 155).

The **Statistics** page displays various statistics to provide an indication that the KServer is running optimally. The statistics shown are not affected by the **machine ID/group ID filter** (page 592) setting.

## System

### Agents currently online

Number of agents currently checking into the system.

### Total Licenses Used

Number of agent licenses used.

### Total Template Accounts

Number of [machine ID templates](#) (page 592) defined.

### Total Machine IDs

Number of machine IDs defined on the KServer, whether their agents have ever checked in or not.  
*Total Licenses Used + Total Template Accounts = Total Machine IDs.*

### KServer CPU usage

the last 5 minutes: x%  
long term average: x%

### Total System CPU usage

the last 5 minutes: x%  
long term average: x%

### Remote Control Sessions

The number of remote control sessions relayed through the KServer that are currently active.

### Pending Alerts

Alerts are processed by the background task every two minutes. This number shows how many alerts are backed up waiting to be processed by your system. If more than 0 alerts are pending, a button appears labeled [Clear Alerts](#) appears. Click this button to clear out all pending alerts.

### Pending Patch Scan Results

The number of machines that currently have patch scan results that have been completed but not yet processed. If a KServer has a lot of patch scans that happen in a short period of time, the actual results of those scans might not appear for some time. The count is a measure of that backlog of processing.

### Database Location

Displays the location of the database.

### Database Size

Total size of your database. Typical systems consume about 1 to 2 MB of database size per machine ID.

### Database File Path

Full path to the database on the database server machine.

### Kaseya File Path

Full path on the KServer to the location of its system files.

### Statistics Collected

[Active connections](#) - Number of managed machines that currently have active connections to the KServer.

**New connections in last 10 seconds** - Number of new TCP/IP connections accepted by the KServer. Agents using a connection established during a prior check-in do not contribute to this count.

**Checkin message queue length** - Number of check-in messages waiting for processing by the KServer.

**Command message queue length** - Number of messages, other than check-in, waiting for processing by the KServer.

**Bandwidth - received bytes/sec** - Bytes per second input into the KServer agent port.

**Bandwidth - sent bytes/sec** - Bytes per second output from the KServer agent port.

**Database CPU utilization** - This number indicates the percentage of CPU utilization by the database server at the time specified. Excessively high values for prolonged periods may be an indication that this server is underpowered or could benefit from additional RAM.

**Total connections processed since KServer start** - This number indicates the total agent connections processed by the KServer since the service last started.

**Event log entries received in last minute** - The number of event log entries received in the last minute for the entire system.

**Event log entries received in last five minutes** - The number of event log entries received in the last five minutes for the entire system.

**Event log entries received in last hour** - The number of event log entries received in the last hour for the entire system.

### Top procedures run in the last hour

This table lists the procedures that have run and completed execution on all online machines in the last hour, with the greatest frequency listed first.

### Top procedures pending (online machines only)

This table lists the procedures waiting to execute on all online machines, with the greatest frequency listed first.

## Logon Policy

### System > Logon Policy

- This page applies to the following product: *On Premises*

The **Logon Policy** page sets logon policies that apply to all VSA users. Logon policies prevent a brute force break-in to the system. By limiting the successive number of bad logon attempts and disabling rogue accounts for a set amount of time, you can prevent unauthorized access achieved by repeatedly entering random passwords.

**Note:** See *VSA Logon Policies (page 388)* for a summary of functions affecting user logons.

### Specify the bad logon attempt policy

- **Number of consecutive failed logon attempts allowed before disabling** - Specify the number of consecutive bad logons a VSA user or **Portal Access (page 81)** user is allowed before their account is disabled in the  account field. The count is reset to zero after a successful logon.
- **Length of time to disable account after max logon failures exceeded** - Specify the amount of time, in hours or days, that the account is disabled in the  field.

**Note:** To activate the account manually before the lockout time elapses, another user must enable the account using the **System > Users (page 397)** page.

## System

- **Minutes of inactivity before a user session expires** - Specify the time period of user inactivity before the user is automatically logged out. Set the number of minutes of inactivity in the  field.
- **Prevent anyone from changing their logon name** - Prevent anyone from changing their logon *name*.
- **Do not show domain on logon page** - Hide the **Domain** field on the logon page.

**Note:** If left blank, the domain checkbox still does not show on the logon page until at least one domain logon exists. Domain logons can be imported using *Agent > View AD Users* (page 66) or added manually using *System > Change Logon* (page 392).

- **Do not show remember me checkbox on logon** - Hide the **Remember my username on this computer** checkbox on the logon page.

## Specify password strength policy

Specify a password strength policy by checking the boxes beside the following:

- **Require password change every N days**
- **Enforce minimum password length**
- **Prohibit password reuse for N passwords**
- **Require upper and lower case alpha characters**
- **Require both alpha and numeric characters**
- **Require non-alphanumeric characters**

## Update

Press **Update** to apply the settings.

## Application Logging

### System > Application Logging

- This page applies to the following product: *On Premises*

The **Application Logging** page controls the logging of application activity on the application server. *This function is only visible to master role users and is used primarily by Kaseya support.*

- It is possible to set the level of logging in the log files, from `None` to `Maximum`. The amount of information in these logs depends on how much logging is in each application and the level of detail specified by the **Application Logging** configuration.
- There are also checkboxes to record the request and response. An XML file is created in `\Kaseya>Xml>Log` for each request and each response. In addition, there is an option to log transactions. When this is checked, another XML file is created in this same directory for each database update.
- There are options to filter by queue. This is to help narrow down the amount of information that goes into the log.
- The **Log** tab displays log records. This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).

## Outbound Email

### System > Outbound Email

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Outbound Email** page maintains settings for routing outbound email generated by the KServer to a host email server. The host email server accepts outbound email and delivers it to recipients on your behalf. If the email server host requires authentication you can include a username and password.

**Note:** These settings are typically set during the install process. You can modify them after the install using this page.

### Enable/Disable Automatic Delivery

Automatic delivery of outbound email is disabled by default. You must enable automatic delivery of outbound email to send emails automatically throughout the VSA as soon as they are created.

### Manual Delivery

If you disable automatic delivery, you can still send outbound email manually:

1. Click the System > Outbound Email > **Log** tab
2. Select one or more outbound emails with a status set to `Queued`.
3. Click the **Send Now** button.

### Configuration

Click **Edit**. Complete the fields in the **Edit** dialog box.

- **Host Name** - The name of the host email server. Example: `smtp.mycompany.com`. If no authentication or special port number is required, then only specify values for the **Default Days to Keep Logs** and **Default Sender Email** fields.

**Note:** Entering `localhost` in the **Host Name** field means you are using the KServer's IIS Default SMTP Virtual Server to route outbound email. The **Default SMTP Virtual Server** service must be installed and running in order to send email. The service must also be able to resolve DNS addresses to route email to other SMTP servers.

- **Port** - Typically 25, but the host email server may require a different port number.
- **User Name** - If required for authentication, enter the username of an account authorized to use the host email server.
- **Password** - If required for authentication, enter the password of the account.
- **Default Days to Keep Logs** - Enter the number of days to keep log outbound email entries.
- **Default Sender Email** - Enter the default From address displayed by outbound email. The From address displayed by outbound email uses the following order of precedence:
  1. If there is a From address in the **Send Email** step of a procedure, then that address is used.
  2. Else the Send Email step uses the From address provided by a linked Service Desk > **Message Template**, if the link exists and a From address is specified.
  3. Else the Send Email step uses the **Reply Email Address** of the Service Desk > **Incoming Email and Alarm Settings** > email reader linked to the service desk. This link between the email reader and the service desk is set using the Service Desk > Desk Definition > Properties > General > Standard Field Defaults > Email field.
  4. Else the **Default Sender Email** address set in System > **Outbound Email** is used.

### Testing

If you suspect that you are not receiving emails from the KServer, click the **Test** button on this page to send test emails to various recipient addresses.

**Note:** If `localhost` is entered in the **Host Name** field, the **Log** tab could show a sent email as successful, but still not be relayed successfully because of configuration problems with the **Default SMTP Virtual Server**.

Click **Test**. Complete the fields in the **Test** dialog box.

- **To** - The email address to send the test email.
- **Subject** - The subject line of the test email.

## Logging

The **Log** tab displays a log of all outbound emails sent by the KServer. This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18).

- **Send Now** - Send or resend selected emails
- **Forward** - Forward a selected email to a different address than originally specified.
- **View** - View a selected email.
- **Delete** - Delete selected emails.

---

# Customize

## Color Scheme

### System > Color Scheme

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Color Scheme** page determines the set of colors displayed by the VSA environment. **Color Scheme** selection is by user and persists between logon sessions.

To change color schemes:

1. Select a color scheme in the middle pane.
2. Click the **Set Scheme** button.

## Site Customization

### System > Site Customization

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Site Customization** page provides the following tabs for customizing the user interface *for all users*.

- **Logon Page** (page 428)
- **Site Header** (page 429)
- **Report Header** (page 430)
- **Agent Icons** (page 429)
- **Org Custom Field Title** (page 430)

Each tab is edited separately.

### Site Customization > Logon Page

The **Logon Page** tab of the **Site Customization** page sets the options displayed when a user logs on.

**Note:** See **VSA Logon Policies** (page 388) for a summary of functions affecting user logons.

1. Click the **Edit** button on the **Logon Page** tab. The **Edit Logon Page** dialog displays.
2. The following settings are all optional:
  - **Logo for Logon Page** - Browse to select a custom logon on your local machine or network.

**Note:** Your logo should be no larger than the recommended size.

- **Title** - Enter title text for this environment. The title displays just beneath the logo on the logon page.
- **Right Frame URL** - Browse to select a custom image on your local machine or network.

- **Display System Version on logon page** - If checked, the system version displays.
- **Display Forgot Password on logon page** - If checked, a **Forgot Password?** hyperlink displays on the logon page. Clicking the **Forgot Password?** link on the logon page—if activated using the System > Site Customization > **Logon Page** (page 428) tab—emails you a link where you can change your password. To change your password, you must have already filled out a **Security Question** and **Security Answer** using System > **Change Logon** (page 392).
- **Display System Status on logon page** - If checked, the system status displays on the logon page.
- **Display Customer ID on logon page** - If checked, the customer ID displays on the logon page.

### Site Customization > Site Header

1. Click the **Edit** button on the **Site Header** tab. The **Edit Site Header** dialog displays.
2. The following settings can be customized:
  - **Logo** - Browse to select a custom logo on your local machine or network. Click the **Default** button to reset back to the default.

*Note: By default, VSA report headers display the image specified by the System > Site Customization > Site Header (page 429). Changing the value in the System > Configure > Change URL... (page 418) > Logo field overrides this default, changing the URL for report headers only. Changing the URL in the Change URL... > Logo field does not affect the display of the Site Header image.*

- **Title** - Enter a custom title that displays next to the logo. Click the **Default** button to reset back to the default.
- **Header Height** - The header height in pixels. Defaults to 50.
- **Favorites Icon** - When your VSA website is bookmarked in a browser, this "favicon" image displays next to the text of the bookmark. Customize this image using a 16x16 pixel ico file.

*Note: The Favorites Icon is not supported in SaaS.*

### Site Customization > Agent Icons

1. Click the **Edit** button on the **Agent Icons** tab. The **Edit Agent Icons** dialog displays.
2. Upload customized Windows icons to the KServer. Windows icons must be in .ico format, the color depth must not exceed 256 colors, and can have a maximum size of 32x32 pixels.
  - **Agent online** - The agent is checking in successfully.
  - **Agent offline** - The agent is not checking in.
  - **Agent blinking** - A message is waiting to be read by the machine user.
  - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.
3. Upload customized Mac icons to the KServer. Mac icons must be in .tif format, the color depth must not exceed 32 bit color, and can have a maximum and recommended size of 48x48 pixels.
  - **Agent online** - The agent is checking in successfully.
  - **Agent offline** - The agent is not checking in.
  - **Agent blinking** - A message is waiting to be read by the machine user.
  - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

*Note: Custom Mac icon images do not display in the Site Customization page, but display correctly when an agent install package is subsequently created and installed on a Mac machine.*

4. Upload customized Linux icons to the KServer. Linux icons must be in .png format, the color depth must not exceed 256 colors, and can have a maximum size of 32x32 pixels.

## System

- **Agent online** - The agent is checking in successfully.
- **Agent offline** - The agent is not checking in.
- **Agent blinking** - A message is waiting to be read by the machine user.
- **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

**Note:** See [Creating Custom Agent Icons](#) (page 430) for more information.

### Site Customization > Deploy Header

Customize the logo and text displayed when Agent > **Deploy Agent** (page 39) displays a web page to the user, instructing them to install the agent.

### Site Customization > Org Custom Field Titles

Customize the titles of custom fields that are used to classify organizations. Assign values to custom fields using System > Manage > Org/Groups/Depts/Staff > **Custom Fields** (page 411).

## Creating Custom Agent Icons

### Four Agent Icons

To incorporate custom agent icons in the system tray (Windows) or menu bar (Mac OS X) of each managed machine, create *four icons*. These icons must be named:

#### For Windows Agents

- `online.ico` – By default, this is the blue K icon  displayed when agent is connected to the KServer.
- `offline.ico` – By default, this is the gray K icon displayed when agent is not connected to the KServer.
- `blink.ico` – By default, this is the white K icon displayed when agent requires the user to click the icon to see a message.
- `noremove.ico` – By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

#### For Mac Agents

- `macOnline.tif` - By default, this is the blue K icon  displayed when agent is connected to the KServer.
- `macOffline.tif` - By default, this is the gray K icon displayed when agent is not connected to the KServer.
- `macNoremove.tif` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message.
- `macBlink.tif` - By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

#### For Linux Agents

- `linuxOnline.png` - By default, this is the blue K icon  displayed when agent is connected to the KServer.
- `linuxOffline.png` - By default, this is the gray K icon displayed when agent is not connected to the KServer.

- `linuxNoremove.png` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message.
- `linuxBlink.png` - By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

### Formatting Custom Agent Icons

For **Windows** custom agent icons:

- The format must use the Windows icon format. A simple bitmap file cannot simply be renamed using the `.ico` extension.
- The size cannot be larger than 32x32 pixels.
- The color depth cannot exceed 8 bit color (256 colors).

For **Macintosh** custom agent icons:

- The format must be `.tif`.
- The recommended size is 48x48 pixels and cannot be any larger.
- The color depth should be RGB 32 bit color.

For **Linux** custom agent icons:

- The format must be `.png`.
- The size cannot be larger than 32x32 pixels.
- The color depth cannot exceed 8 bit color (256 colors).

### Installing Custom Icons

1. Navigate to the System > Site Customization > **Agent Icons** (page 429) tab.
2. Click the **Agent Icons** tab.
3. Click the **Edit** button. The **Edit Agent Icons** dialog displays.
4. Click the browse button for any agent icon to select a custom agent icon on your local machine.
5. Optionally click the **Use Default** buttons to reset agent icons to their default images.

### Updating Existing Agents with Custom Agent Icons

The customized agent icons are automatically deployed when updating Agents using the Agent tab -> **Update Agent** (page 84). You will need to check the **Force update** check box to update agents that are already at the current version.

### Creating Agent Install Packages with Custom Agent Icons

Updated agent icons are included in any newly downloaded `KcsSetup` files created by **Deploy Agent** (page 39). If you have placed an agent installer `KcsSetup` file in a domain logon script, then you must re-download the `KcsSetup` file to include the updated icons and replace the file on the domain server.

## Local Settings

### System > Local Settings

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The following settings will be applied system wide going forward from this release. These settings currently affect the **Time Tracking** and **Service Billing** modules.

### Date Format

- **Format** - Selects the date format used by dates the VSA.
  - `mm/dd/yyyy`
  - `dd/mm/yyyy`
  - `yy/mm/dd`

## System

- **Delimiter used** - Selects the date format delimiter used by dates in the VSA.
  - / (slash)
  - - (dash)
  - . (dot)

## Number Format

- **Decimal Places** - Selects the number of decimal places used to display currency in the VSA.
- **Decimal Format** - Selects the decimal format used to display currency in the VSA.
  - xx,xxx.xx
  - xx.xxx,xx

## Customize: Live Connect

### System > Customize > Live Connect

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Customize: Live Connect** page customizes **Home** tabs that display in the **Live Connect** (page 380) and **Portal Access** (page 81) windows. You can create multiple, customized **Home** tabs and save them by name.

These **Home** tabs are enabled for a particular role by checking the checkbox underneath Live Connect > Home in:

- System > User Roles > **Access Rights** (page 401)
- System > Machine Roles > **Access Rights** (page 403)

**Note:** You can download a Live Connect PDF from the first topic of online help.

You can customize three sections on the default **Home** page.

- **Portal Header** - Customize the text and image displayed at the top of the **Home** tab.
- **Agent Procedures** - Provide a customized list of agent procedures that the user can run immediately from this tab.
- **Custom Links** - Provide a customized list of URLs that the user can click using this tab. For example, you could provide a URL to a website page providing technical information used to troubleshoot problems on managed machines.

## Make available to All Tenants

If checked, this Home page can be added to user roles and machines roles on all tenant partitions. This option only displays for **master role users** (page 600).

## Chapter 11

# Ticketing

### In This Chapter

Ticketing Overview	435
View Summary	435
Create/View	438
Delete/Archive	441
Migrate Tickets	443
Notify Policy	443
Access Policy	445
Assignee Policy	446
Due Date Policy	447
Edit Fields	448
Email Reader	449
Email Mapping	451

## **Ticketing**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

## Ticketing Overview

The **Ticketing** module manages service requests. These service requests, and your response to them, are documented using **tickets**.

The ticketing system automatically notifies designated VSA users and ticket submitters by email for such system events as ticket creation, changes, or resolutions. The system organizes tickets by machine ID, group ID, organization ID, department ID or staff ID. You may wish to create a "generic" organization in System > **Manage** (page 408) to hold tickets of a global nature, such as general network problems.

### Visibility of Tickets in Other Modules

Tickets can also be viewed using **Live Connect** (page 380) and in Info Center > **View Dashboard** (page 180).

Functions	Description
<b>View Summary</b> (page 435)	Lists all tickets. Each row displays summary data for a single ticket.
<b>Create/View</b> (page 438)	Create new tickets, or add or modify notes in existing tickets.
<b>Delete/Archive</b> (page 441)	Permanently delete tickets or move tickets into archival storage.
<b>Migrate Tickets</b> (page 443)	Migrate Ticketing tickets to and from Service Desk tickets.
<b>Notify Policy</b> (page 443)	Determine when email notifications are sent out by the Ticketing module.
<b>Access Policy</b> (page 445)	Determine who can edit and/or display fields in tickets.
<b>Assignee Policy</b> (page 446)	Create policies to automatically assign users to a new or existing ticket.
<b>Due Date Policy</b> (page 447)	Define default due dates for new tickets based on field values and email subject lines.
<b>Edit Fields</b> (page 448)	Define, modify, or create ticket fields used to classify tickets.
<b>Email Reader</b> (page 449)	Setup automatic polling of a POP3 email server to generate new ticket entries.
<b>Email Mapping</b> (page 451)	Define default field values for new tickets received using the Email Reader.

---

## View Summary

Ticketing > View Summary

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT

## Ticketing

### Workbench

- Similar information is provided using [Info Center > Reports > Ticketing \(page 176\)](#).

The [View Summary](#) page lists all tickets. Each row displays summary data for a single ticket.

## New Tickets or New Notes

New tickets, or new notes in existing tickets, are clearly highlighted in one of two ways.

- **By Date** - Tickets with new notes entered in the last 1 day are **highlighted in red**. New notes entered in the last 7 days are **highlighted in yellow**. You can adjust these times and colors by clicking the [Change Highlight](#) link.
- **Read Flag** - Each ticket is flagged to indicate if the user has viewed all the notes in the ticket. Once viewed, the ticket is marked as read using the  icon. If another user or user adds or modifies a note, the flag is switched back to unread for you, showing the  icon.

## Filtering

The list of tickets displayed depends on several factors:

- The list displayed depends on the [machine ID / group ID filter \(page 26\)](#) and machine groups the user is authorized to see using [System > Scope \(page 404\)](#).
- You can further *sort* and *filter* listed tickets by selecting values in the field drop-down lists.
- **Search** does not display any tickets if notes contain none of the words being searched for.
- Machine users only have access to tickets for their own machine ID using [Portal Access \(page 81\)](#).

## Assignees

The assignee list displayed in [View Summary \(page 435\)](#) and [Create/View \(page 438\)](#) is based on the scope of the currently logged on user. Ticketing assignment in the [Ticketing](#) module always allows you to see master users, regardless of your role or scope.

## Open Tickets, Past Due, Closed Tickets, Total Tickets

Shows the number of tickets open, past due, closed, and total for all tickets matching the filtering criteria described above.

## Search

**Search** restricts the list of tickets to only tickets containing **any** of the words or phrases in the search string. Enclose a phrase in double-quotes ("). Search examines the ticket [Summary](#) line, submitter [Name](#), submitter [Email](#), submitter [Phone](#), or any of the [Notes](#).

Clicking any of the ticket [Summary](#) links in the paging area displays the details of that ticket using the [View Ticket \(page 438\)](#) page. Words in the ticket notes matching any **Search** word are *highlighted with a green background*.

## <last 10 searches>

The drop-down list below the [Search](#) edit box lists the <last 10 searches> you have made. Selecting any item from the list automatically re-searches for those words.

## Sort

Click either [ascending](#) or [descending](#) to order tickets by the selected column.

## Fields...

Allows each user to organize the columns displayed in the table. Clicking [Fields...](#) opens a dialog in a new browser window. There, you can select which columns to show or hide and also the order in which columns are displayed. You can show/hide any of the following columns:

- **ID** - Unique ID number automatically assigned to each ticket.

- **Machine ID** - The ticket applied to this machine.
- **Assignee** - Name of the user responsible for solving this problem.
- **Category** - Type of problem this ticket discusses.
- **Status** - Open, Hold, Closed
- **Priority** - High, Normal, Low
- **SLA Type** - Service Level Agreement type
- **Dispatch Tech** - Yes, No
- **Approval** - Required, Not Required
- **Hours Worked** - Hours worked, in decimal format.
- **Last Modified Date** - Last time any note was added to this ticket.
- **Creation Date** - Time when the ticket was first entered.
- **Due Date** - Ticket due date.
- **Resolution Date** - Date the ticket was closed.
- **Submitter Name** - Person who submitted this ticket: user, user name, or machine ID.
- **Submitter Email** - The submitter email address.
- **Submitter Phone** - The submitter phone number.

You can also select additional custom fields you have previously created using Ticketing > [Edit Fields](#) (page 448).

### Automatically submit on field changes / Submit

If **Automatically submit on field changes** is checked, then the **View Summary** page redisplay as soon as a single field in the **List Fields Filter** is changed. If blank, then you can change several of the **List Fields Filter** at one time. The **View Summary** page won't redisplay until you click **Submit**.

### (List Fields Filter)

Each field of type `List`—such as **Category**, **Status**, or **Priority**—are shown as selectable drop-down lists. Selecting values from one or more of these drop-down lists filters the paging area to display only those tickets matching the selected values. Custom `List` fields are created using Ticketing > [Edit Fields](#) (page 448).

### Mark All Read

Click to mark all tickets as read. Read tickets display a  icon. Any changes or note additions inserted by other users reset the ticket to unread. Unread tickets display a .

### Set Field...

Use **Set Field...** to change multiple field values on multiple tickets at once. Check the box for all the tickets you wish to change a field value for. Then click **Set Field...** A dialog box displays that enables you to set a new value for any of the fields.

### Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

### Merge...

To merge tickets, *check the box for any two tickets* listed, then click the **Merge...** button. The resulting merged ticket contains all the notes and attachments from both tickets. You are asked which field values you wish to use in the ticket for all field values that are different between the two tickets.

## Ticketing

### Change Highlight

Click **Change Highlight** to set and/or modify row highlighting based on date. Highlight tickets in two ways. Tickets with a date within 1 day of the current time are **highlighted in red**. Tickets with a date within 7 days are **highlighted in yellow**. You can independently *adjust both the number of days and the highlight color*. To disable highlighting by date, set each number of days to zero. The highlight date may be **last modified date**, **due date**, or **creation date**.

### Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

### Column Headings

Clicking any column heading re-orders the table using that column as the sort criteria.

### Data Table

Each row of the table lists summary data for a single ticket.

- To display the details of the ticket in a *new window* click the new window  icon. Hovering the mouse cursor over the  icon of a ticket displays a preview window of the latest notes for that ticket. Use this to quickly review tickets in your queue. The number of milliseconds the cursor has to hover can be specified using System > **Preferences** (page 391).
- To display the details of the ticket in the *same window* click the **summary** line link.
- To toggle the state to *read* click .
- To toggle the state to *unread* click .

---

## Create/View

### Ticketing > Create/View

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Create/View** page creates new tickets, or adds or modify notes in existing tickets.

### Adding a New Ticket

1. Bypass the **Ticket ID** field. It will be populated with a new unique number when the ticket is created.
2. Click **Select association** to associate the ticket with one of five types of VSA records: machine ID, machine group, organization, department, or staff. This is mandatory.
3. Enter a short description of the problem in the **Summary** field.
4. The **Submitter** fields are populated as follows:
  - If a machine ID was selected in step 2, the submitter **User Name**, **User Email** and **User Phone** fields are populated with contact data maintained for this machine ID using Agent > **Edit Profile** (page 79). This information can be updated if need be.
  - If anything other than machine ID was selected in step 2, these submitter fields can be filled in manually, if applicable.
  - If a ticket was created by an incoming email using Ticketing > **Email Reader** (page 449), the **Submitter Email** field is populated with the sender's email address.
5. The **Date Created** is automatically assigned.
6. The **Age / Closed** date is automatically assigned. **Age** lists the number of hours/days since the creation date for non-closed tickets. If the ticket has been closed then **Age** is replaced with **Closed** and displays the date and time this ticket was closed.

7. The default due date for a ticket is determined by the Ticketing > **Due Date Policy** (page 447). The due date is based on the ticket attributes you enter when a *new* ticket is entered. If a due date policy is in force for a ticket, then a policy icon  displays next to the due date. You can override the existing due date by clicking the edit icon  next to the due date. The policy icon  is replaced by a manual override icon  next to the due date. Click the **Apply** button to reset the due date to the policy enforced due date. If the due date does not match any of the defined **due date policies** (page 447), then the **Due Date** label is highlighted. If no due date policies are defined then the system default due date is used, which is one week from the creation date of the ticket. When a ticket is overdue, the due date displays in bolded **dark red text**, both in the **View Summary** (page 435) page and in **Ticketing** (page 176) reports. It also displays in **red text** in the header of the **Create/View** (page 438) page. You can optionally send an email for overdue tickets using Ticketing > **Notify Policy** (page 443). A ticket is resolved when its status is set to closed and the resolution date is recorded.
8. Classify the ticket using the built-in **List** type fields, such as **Assignee**, **Category**, **Status**, and **Priority**. You can also classify the ticket using additional **List** type fields that have been created for tickets using Ticketing > **Edit Fields** (page 448).
9. Enter details of the problem in the **Notes** edit box. Click the **Note Size** link to change the number of rows available for your note text.
10. To attach a file, such as a screen shot, to the ticket, click **Browse...** below the note entry area. Locate the file you wish to attach on your local computer. Click **Open** in the browse window to upload the file to the VSA server. Once the file has been successfully uploaded, tag text is automatically entered into the note in this format: `<attached file:filename.ext>`. This tag appears as a hyperlink in a note for the ticket. Display/download the file at any time by clicking that link.
 

**Note:** The following list of filename extensions display as images or text in the note, instead of displaying as a hyperlinked filename: gif, jpg, png, bmp, txt, sql.

**Note:** Ticket note attachments are typically located in the `C:\Kaseya\WebPages\ManagedFiles` directory.
11. Check the **Suppress email notification** checkbox if you don't want email recipients, either VSA users or machine users, to be notified about the ticket. In most cases you'll want to leave this blank.
12. Check the **Suppress automatic note creation checkbox** if you don't want a note to be added automatically. This option is hidden by default. Use **Access Policy** (page 445) to display it.
13. Complete the creation of the ticket in one of two ways:
  - Click **Submit** to complete the creation of the ticket and to notify *both* VSA users and machine users by email.
  - Click **New Hidden** to complete the creation of the ticket to notify *only* VSA users by email. Use hidden notes to record data or analysis that may be too detailed or confusing to machine users but useful to other VSA users.

**Note:** Hidden notes are *never* included in email notifications.

## Editing an Existing Ticket

To display an existing ticket, enter a ticket number in the **Ticket ID** field.

- If you don't know the number of the ticket, use **View Summary** (page 435) or **Delete/Archive** (page 441) to locate and select the ticket. The ticket will be displayed using this page.
- When an existing ticket first displays on this page, the header fields show the most recent settings for the ticket.
- Making changes to any of the **List** type fields immediately creates a new note for the ticket, identifying the change.
- Making changes to any of the non-**List** type fields—such as the **Summary** field, **Submitter** information, or fields that accept freeform text entries or numbers—requires you to click **Update** afterwards to create a new note.

## Ticketing

- Edit any *previous* note for a ticket by clicking the edit icon  next to the note you wish to edit. This populates the header fields with the settings for this note. It also highlights the row of the note being edited in light yellow. You can change the contents of the note, including the timestamp for the note. Click **Change** to confirm the changes you have made.
- Delete notes by clicking the delete  icon next to the note.
- Split a ticket into two tickets by clicking the split  icon next to the note. The new ticket contains the note and all more recent notes. The original ticket can either be closed or left unchanged.

**Note:** View, edit and delete privileges for tickets and fields are controlled using [Ticketing > Access Policy \(page 445\)](#). VSA users and machine users are notified about ticket changes based on [Ticketing > Notify Policy \(page 443\)](#). Change the number automatically assigned to the next new ticket using [Edit Fields \(page 448\)](#).

## Assignees

The assignee list displayed in [View Summary \(page 435\)](#) and [Create/View \(page 438\)](#) is based on the scope of the currently logged on user. Ticketing assignment in the **Ticketing** module always allows you to see master users, regardless of your role or scope.

## Assignee Policy Icon

By default a `always enforce assignee policy` icon  displays next to the assignee field. This indicates that assignee names are automatically selected using [Assignee Policy \(page 446\)](#). Click the  icon once to display the `override the assignee policy` icon . This overrides the assignee policy and allows you to select an assignee manually.

**Note:** If no assignee policy is defined for the combination of `List` type fields values selected, then toggling between the  and  icons has no effect.

## Displaying the "Create/View" Page Using a URL

The following URL displays the [Create/View \(page 438\)](#) web page for a specific ticket ID

```
http://...?tucid=<TicketID>
```

For example:

```
http://demo.kaseya.com?tucid=1234
```

## Time/Admin

Lists the time a change was made to a ticket and the user or user who made the change.

## Note

Lists all notes relating to this ticket in ascending or descending time order. Each note is time stamped and labeled with the logon name of the person entering the note.

**Note:** User entered notes are labeled with the machine ID they logged in with. See [Portal Access \(page 81\)](#) for details.

## Hide

If checked, the note is hidden from VSA users but not machine users. The default setting is determined by the `as hidden note` checkbox in [Ticketing > Access Policy \(page 445\)](#). Access policies are applied by user role. If you belong to more than one user role, the most restrictive policy has precedence.

---

# Delete/Archive

## Ticketing > Delete/Archive

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Delete/Archive** page deletes old tickets, or deletes tickets in a particular category or status. You may reach the point where your system has so many old tickets that they are cluttering up searches with obsolete data.

**Note:** View, edit and delete privileges for tickets and fields are controlled using [Ticketing > Access Policy](#) (page 445).

## Archiving Tickets

In addition to delete, you can also **archive** tickets. Archived tickets stay in the database but are moved to separate tables. Use archive to move obsolete or old tickets out of the active database **without** deleting them from the system. You can always move tickets back and forth between the active database table and the archive database table.

## Filtering

The list of tickets displayed depends on several factors:

- The list displayed depends on the **machine ID / group ID filter** (page 26) and machine groups the user is authorized to see using System > **Scope** (page 404).
- You can further *sort* and *filter* listed tickets by selecting values in the field drop-down lists.
- **Search** does not display any tickets if notes contain none of the words being searched for.
- Machine users only have access to tickets for their own machine ID using **Portal Access** (page 81).
- Use the **Hide tickets last modified after** control to only display tickets *earlier* than a certain date.

## Archiving Closed Tickets

If, for example, you want to archive **Closed** tickets older than 6 months perform the following steps:

1. Select **Closed** from the **Status** control.
2. Set the **Hide tickets last modified after** control to list only tickets last modified 6 months ago or earlier.
3. Click the **Set** button.
4. Click the **Select All** link.
5. Click the **Archive...** button.
6. Check the **Display archived tickets instead of active tickets** checkbox to search and examine the archived tickets. You can move tickets back to the active table here using the **Restore...** button.

## Open Tickets, Past Due, Closed Tickets, Total Tickets

Shows the number of tickets open, past due, closed, and total for all tickets matching the filtering criteria described above.

## Search

**Search** restricts the list of tickets to only tickets containing **any** of the words or phrases in the search string. Enclose a phrase in double-quotes ("). Search examines the ticket **Summary** line, submitter **Name**, submitter **Email**, submitter **Phone**, or any of the **Notes**.

Clicking any of the ticket **Summary** links in the paging area displays the details of that ticket using the **View Ticket** (page 438) page. Words in the ticket notes matching any **Search** word are *highlighted with a green background*.

## Ticketing

### <last 10 searches>

The drop-down list below the [Search](#) edit box lists the <last 10 searches> you have made. Selecting any item from the list automatically re-searches for those words.

### Sort

Click either [ascending](#) or [descending](#) to order tickets by the selected column.

### Fields...

Allows each user to organize the columns displayed in the table. Clicking [Fields...](#) opens a dialog in a new browser window. There, you can select which columns to show or hide and also the order in which columns are displayed. You can show/hide any of the following columns:

- [ID](#) - Unique ID number automatically assigned to each ticket.
- [Machine ID](#) - The ticket applied to this machine.
- [Assignee](#) - Name of the user responsible for solving this problem.
- [Category](#) - Type of problem this ticket discusses.
- [Status](#) - Open, Hold, Closed
- [Priority](#) - High, Normal, Low
- [SLA Type](#) - Service Level Agreement type
- [Dispatch Tech](#) - Yes, No
- [Approval](#) - Required, Not Required
- [Hours Worked](#) - Hours worked, in decimal format.
- [Last Modified Date](#) - Last time any note was added to this ticket.
- [Creation Date](#) - Time when the ticket was first entered.
- [Due Date](#) - Ticket due date.
- [Resolution Date](#) - Date the ticket was closed.
- [Submitter Name](#) - Person who submitted this ticket: user, user name, or machine ID.
- [Submitter Email](#) - The submitter email address.
- [Submitter Phone](#) - The submitter phone number.

You can also select additional custom fields you have previously created using Ticketing > [Edit Fields](#) (page 448).

### Automatically submit on field changes / Submit

If [Automatically submit on field changes](#) is checked, then the [View Summary](#) page redisplay as soon as a single field in the [List Fields Filter](#) is changed. If blank, then you can change several of the [List Fields Filter](#) at one time. The [View Summary](#) page won't redisplay until you click [Submit](#).

### (List Fields Filter)

Each field of type `List`—such as [Category](#), [Status](#), or [Priority](#)—are shown as selectable drop-down lists. Selecting values from one or more of these drop-down lists filters the paging area to display only those tickets matching the selected values. Custom `List` fields are created using Ticketing > [Edit Fields](#) (page 448).

### Hide tickets last modified after / Set

[Set](#) the date and time of this control to only display tickets *earlier* than a certain date.

### Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

## Delete...

Select one or more tickets and click the [Delete...](#) button to permanently delete the tickets from the system. Deleted tickets cannot be restored.

## Archive...

Select one or more tickets and click the [Archive...](#) button. Archived tickets stay in the database but are moved to separate tables. Use archive to move obsolete or old tickets out of the active database *without* deleting them from the system. You can always move tickets back and forth between the active database table and the archive database table.

## Display archived tickets instead of active tickets / Restore

Check the [Display archived tickets instead of active tickets](#) checkbox to search and examine the archived tickets. You can move tickets back to the active table here using the [Restore...](#) button.

---

# Migrate Tickets

## Ticketing > Migrate Tickets

- This page applies to the following products: On Premises, Kaseya Advanced

The [Migrate Tickets](#) page performs two tasks:

- Migrates selected [Ticketing](#) tickets into [Service Desk](#) tickets.
- Imports [Service Desk](#) ticket XMLs into [Ticketing](#) tickets.

## Migrating Tickets from Ticketing into Service Desk

The paging area of [Migrate Tickets](#) displays all the tickets visible to you in the Ticketing > [View Summary](#) (page 435) page.

1. Select the tickets you want to migrate in the paging area. Click [Select All](#) to select all tickets.
2. Click [Migrate](#) to migrate all the selected tickets into [Service Desk](#).

## Importing Service Desk Tickets into Ticketing

1. Export selected tickets in [Service Desk](#) to an XML file on your local machine or network, using the [Export](#) button in Service Desk > [Tickets](#).
2. Click [Import](#) in Ticketing > [Migrate Tickets](#) and select the XML file you created in step 1 above.

---

# Notify Policy

## Ticketing > Notify Policy

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The [Notify Policy](#) page determines when email notifications are sent out by the [Ticketing](#) module. *Multiple policies can be defined for each machine group, by clicking the [Add](#) button instead of the [Update](#) button.* This lets you specify different email lists for different ticketing events. For example, you may wish to send email alerts to a group of users for ticket creations and note additions, but send email to a

## Ticketing

different list of users for overdue tickets.

To be sent email notification for a ticketing event:

1. Check the box to the left of each ticketing event you need to be notified about.
2. Enter a comma separated list of email address in the **Email List** edit box.
3. Check the box to the left of all group IDs you wish to apply this notification policy to.
4. Click the **Update** or **Add** button.

**Note:** You can *not* send notifications to the email address used to receive tickets, defined using Ticketing > **Email Reader** (page 449).

## From Address

The **From** address used by ticket notifications is based on the **Email Reader** (page 449) address, if one is defined. If an **Email Reader** has not yet been defined then the **From** address in System > **Outbound Email** (page 426) is used.

## Notification Type Checkbox

The list below describes when the ticketing system sends an email notification *to all email recipients in the email list*.

- **Ticket Creation** - If checked, an email is sent at the time of ticket creation.
- **Modify/Add Note** - If checked, an email is sent when a ticket is changed, including adding a note to ticket.
- **Overdue Ticket** - If checked, an email is sent when a ticket passes its due date without being closed.
- **Edit Summary** - If checked, an email is sent when anyone changes the summary line for a ticket. Click **Format** to edit the format for this email notification.
- **Send auto response to emails creating new tickets** - If checked, an automated reply message is sent out to the person that sent in an email that generated a new ticket. Automated response emails give your users an acknowledgement that their request has been received and processed by the system. Creating tickets based on inbound emails are configured using **Email Reader** (page 449) and **Email Mapping** (page 451). Click **Format** to edit the format for this email notification.
- **Assignee Change** - If checked, an email is sent when a ticket is assigned to a different user. Click **Format** to edit the format for this email notification.
- **Field Change** - If checked, an email is sent when anyone changes any custom field in a ticket. Click **Format** to edit the format for this email notification.
- **Due Date Change** - If checked, an email is sent when anyone changes the due date of a ticket. Click **Format** to edit the format for this email notification.
- **Notify Ticket Submitter when note added** - If checked, an email is sent to the email address entered for the ticket submitter, in addition to the email list for all email notification messages.
- **Include all public notes in Modify/Add notification** - If checked, *all* notes for a ticket are included when a **Modify/Add Note** message is sent out.
- **Received email alerts always sent to assignee** - If checked, an email is sent to the ticket assignee, whenever a reply email is received and added to the ticket, even if the assignee is not on the notification email list for this group ID.
- **Send auto response to emails creating new tickets** - If checked, an automated reply message is sent out to the person that sent in an email that generated a new ticket. Automated response emails give your users an acknowledgement that their request has been received and processed by the system. Creating tickets based on inbound emails are configured using **Email Reader** (page 449) and **Email Mapping** (page 451). Click **Format** to edit the format for this email notification.

**Note:** Format Email... buttons only display for master role users.

## Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

## Machine Group

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

## Enable Events TMOAFEDNIRS

Identifies the ticketing events that trigger email notification of email recipients listed in the [Email List](#) column.

## Email List

The list of email recipients notified by selected ticketing events for this group ID.

---

# Access Policy

### Ticketing > Access Policy

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Access Policy](#) page determines who can edit and/or display fields in tickets. Independent policies can be set for each user role and for all machine users. Machine users only see tickets assigned to their machine ID. Non-master role users only see tickets for scopes they are authorized to access.

## Select user or user group

Before setting any other policy options, select `<Users>`, meaning all machine users, or a user role from the drop-down list.

## Access Rights

The following access rights apply to *all machine users* or to a selected *user role*, as specified using [Select user or user group](#).

- **Enable ticket delete** - If checked, the selected user role can delete entire tickets using the [Delete/Archive \(page 441\)](#) page.
- **Enable ticket edit to modify or remove notes or modify summary line (Adding new notes is always enabled)** - If checked, the selected user role can edit existing notes or modify the summary line.

**Note:** Adding new notes is always enabled for all user groups.

- **Enable associate ticket with editing** - If checked, enables the selected user role to edit the machine ID or group associated with a ticket.
- **Enable submitter information editing** - If checked, enables submitter information to be edited.
- **Enable due date edit when editing trouble tickets** - If checked, the selected user role can modify the ticket due date.
- **Enable suppress email notifications when editing trouble tickets** - If checked, the selected user role can suppress email notifications when modifying an existing ticket.
- **View hidden notes** - If checked, the selected user role can view hidden notes.

**Note:** Hidden notes can *never* be viewed by users.

## Ticketing

- **Change hidden notes status checkbox** - If checked for the selected user role, notes display a **Hide** checkbox at the far right edge of each ticket note. Toggling the **Hide** checkbox makes a note hidden or not hidden.
- **Automatically insert new note with every field change** - If checked for the selected user role, notes are automatically inserted whenever any ticket field changes.
  - **As hidden note** - If checked for the selected user role, automatic notes are added as hidden notes. This policy only applies if **Automatically insert new note with every field change** is checked.
  - **Allow admin to suppress auto note add** - Suppresses the adding of an automatic note when ticket properties are changed and no manual note is added.
- **Define access to each ticket field** - Defines access to each field for the selected user role. Fields are created using **Edit Fields** (page 448). Three levels of access are possible:
  - **Full Access** - Can view and modify this field in every ticket.
  - **View Only** - Can see but not change the value of this field.
  - **Hidden** - Hidden fields are not shown.

---

## Assignee Policy

### Ticketing > Assignee Policy

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Assignee Policy** page automatically assigns a VSA user to a new or existing ticket. Assignment is based on the combination of `List` type field values entered for a ticket. `List` type fields and their possible values are defined using Ticketing > **Edit Fields** (page 448). The policy is enforced every time the ticket is saved.

### Overriding Assignee Policy

**Assignee Policy** can be overridden for a specific ticket using the **Create/View** (page 438) page, by the toggling the  icon next to the **Assignee** field to display a  icon, then assigning a user manually.

### Order of Precedence

The order of precedence for policy *selection* is based on the alphabetical sort order of the policy *name*, which also determines how the policies are listed in the paging area. For example, a policy named of `AAA` will always be selected before `BBB`, so long as all of the fields in `AAA` match the settings of the ticket. You can *force* policy selection to use the sort order you prefer by naming the policies accordingly. For example, you can add a numerical prefix to each policy name, such as 01, 02, 03, ... and adjust the sort order in this fashion. To rename existing policies, select the edit icon  next to a policy name, then enter a new name and click **Apply**.

### Policy Name

Enter the name for the assignee policy.

### Assignee

Select the user who will be assigned tickets that match the selected combination of `List` type field values.

### Create

Click **Create** to create the assignee policy.

## List Fields

Each field of type `List`—such as **Category**, **Status**, or **Priority**—are shown as selectable drop-down lists. Select values for one or more of the fields. The combination of `List` type field values associated with an assignee determines which assignee is automatically assigned to a new or existing ticket.

---

# Due Date Policy

## Ticketing > Due Date Policy

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The **Due Date Policy** page sets the due date for each **new ticket** based on field values. Any combination of `List` type fields may be defined to set a due date. This allows you to set a new ticket due date based on the urgency of the ticket and a guaranteed level of service. For example, define a new `List` type field named **Service Level** with the following values: *Premium, Standard, Economy*. Create different due date policies for each combination such as:

- Set resolution time to `1 Hrs` when **Priority** = *High* and **Service Level** = *Premium*
- Set resolution time to `7 Days` when **Priority** = *Normal* and **Service Level** = *Economy*

When a new ticket gets created, the due date is set by adding the number of hours in the policy to the current time.

**Note:** You can change the due date of an existing ticket manually using **Create/View** (page 438).

## Overdue Tickets

When a ticket is overdue, the due date displays in bolded **dark red text**, both in the **View Summary** (page 435) page and in **Ticketing** (page 176) reports. It also displays in **red text** in the header of the **Create/View** (page 438) page. You can optionally send an email for overdue tickets using Ticketing > **Notify Policy** (page 443). A ticket is resolved when its status is set to closed and the resolution date is recorded.

## Order of Precedence

The order of precedence for policy *selection* is based on the alphabetical sort order of the policy *name*, which also determines how the policies are listed in the paging area. For example, a policy named of *AAA* will always be selected before *BBB*, so long as all of the fields in *AAA* match the settings of the ticket. You can *force* policy selection to use the sort order you prefer by naming the policies accordingly. For example, you can add a numerical prefix to each policy name, such as *01, 02, 03, ...* and adjust the sort order in this fashion. To rename existing policies, select the edit icon  next to a policy name, then enter a new name and click **Apply**.

## Default time to resolve tickets with no policy

Enter the number of hours or days to resolve tickets when new tickets are created that do not match any policy.

## Policy Name

Enter a name for a new or selected due date policy.

## Resolve Time

When new tickets are created that match the field values in this policy, then the due date is set to this number of hours or days plus the current time.

## Ticketing

### Fields

Select values for one or more `List` type fields that a new ticket must match to automatically set the due date for the new ticket.

### Delete Icon

Click the delete icon  to delete a row in the paging area.

### Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them. The selected row is highlighted in yellow.

### Name

The name of the due date policy.

### Time

The time added to the current date and time to set the due date policy for a new ticket.

### All Other Columns

The values of list fields that must be matched to set a due date for a new ticket using this policy. User defined `List` fields are maintained using [Edit Fields](#) (page 448).

---

## Edit Fields

### Ticketing > Edit Fields

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench*

The [Edit Fields](#) page creates fields used to classify tickets and sets the default values for those fields. Fields are associated with the entire ticket, as opposed to each note of the ticket. You can *customize* the field label and corresponding values of each field, including the mandatory fields. The fields you define here display in the following pages: [View Summary](#) (page 435), [View Ticket](#) (page 438), [Delete/Archive](#) (page 441), [Access Policy](#) (page 445), [Due Date Policy](#) (page 447) and [Email Mapping](#) (page 451).

### Mandatory Fields

Three mandatory `List` type fields exist that may not be removed from the system. The values for these list fields can be customized. The mandatory fields are:

- [Category](#) - Classifies tickets by IT category.
- [Status](#) - State of the current ticket: `Open`, `Hold`, `Closed`
- [Priority](#) - `High`, `Normal`, `Low`

### Set the next ticket ID to N / Apply

Specify the ticket number for the next ticket. Displays the current "next" ticket number. Click [Apply](#) to confirm any changes.

### Field Position

Click the up/down arrows  to the left of the field label to change the display position for this field in [Create/View Tickets](#) (page 438).

## Field Label

You can modify the label for any field here. Click the [Update](#) button to apply the change.

## Type

Specify the data type for each field.

- `String` - Can contain any text up to 500 characters in length. Best used to hold things like problem location or other variables that do not belong in the summary line.
- `Integer` - Can contain any positive or negative integer value
- `List` - Lets you create a drop-down list of choices. The choices for `List` type fields are edited by clicking the `<Edit List>` value in the [Default Value](#) drop-down list.

**Note:** Only `List` type fields display as a selectable drop-down list that can filter the display of tickets in the [View Summary](#) (page 435) and [Delete/Archive](#) (page 441) pages.

- `Number (nn.d)` - A number that always shows one digit to the right of the decimal point.
- `Number (nn.dd)` - A number that always shows two digits to the right of the decimal point.
- `Number (nn.ddd)` - A number that always shows three digits to the right of the decimal point.
- `Number (nn.dddd)` - A number that always shows four digits to the right of the decimal point.

## Default Value

Creating a new ticket automatically sets each field to its default value. You can specify that default value here.

**Note:** Default values are system wide and may not be different for different machine group IDs or user roles.

**Note:** [Email Mapping](#) (page 451) can override the default values selected here for tickets created using [Email Reader](#) (page 449).

## <Edit List>

This value displays in the drop-down list for a `List` type field in the [Default Value](#) column. Click `<Edit List>` to edit the list of values for that field.

## Update

Click [Update](#) to confirm changes to field labels, default values, or `List` type values.

## New

Click [New](#) to create a new field.

---

# Email Reader

## Ticketing > Email Reader

- This page applies to the following products: *On Premises*, *Kaseya Advanced*, *Kaseya Essentials*, *IT Center*, *IT Workbench*

The [Email Reader](#) page specifies a POP3 email account to periodically poll. Email messages retrieved from the POP3 server are classified by [Email Mapping](#) (page 451) and converted into tickets.

## Ticketing

### Alarm to Ticket Integration

When a VSA user clicks a [New Ticket...](#) link—typically for an alarm—anywhere in the system, the **Ticketing** module converts it into a ticket. The **Ticketing** email reader does not have to be enabled.

**Note:** If the **Service Desk** module is installed, see [Service Desk > Activating Service Desk Integration](#).

### Contents of Email

The **Email Reader** can receive any email, with or without attachments, and add the contents to the ticketing system. Additional information can be added to the email to enhance the mapping of the email to the ticketing system. The following tags can be included in *either the subject or the body* of the email.

- `~ticrefid='xxx'` - Appends the body of the email to an existing ticket rather than cause a new ticket to be created.
- `~username='xxx'` - Automatically inserts the value given as `xxx` into the **Submitter Name** field.

**Note:** If `~username='xxx'` is *not* included in the either the subject or the body of the email, then the email sender's **From** address is used to populate the **Submitter Name** field.

- `~useremail='xxx'` - Automatically inserts the value given as `xxx` into the **Submitter Email** field.
- `~userphone='xxx'` - Automatically inserts the value given as `xxx` into the **Submitter Phone** field.
- `~category='xxx'` - Assigns the ticket created to a specific category. The category must exist.
- `~priority='xxx'` - Assigns the ticket created to a specific priority. The priority must exist.
- `~status='xxx'` - Assigns the ticket created to a specific status. The status must exist.
- `~assignee='xxx'` - Assigns the ticket created to a specific user. The user must exist.
- `~machineid='xxx.xxx'` - Assigns the ticket created to a machine ID. The machine ID must exist. If this information is not included, and tickets are not assigned to a machine ID or group ID using **Email Mapping** (page 451), tickets are assigned to the `unnamed` group by default.
- `~fieldName='xxx'` - Assigns the value `xxx` for any defined field. If the field is a `List` type, then the value must exist in the list.

### Suppressed Notes

Notes are suppressed if an email is sent with no body and no attachments or if no response text is sent with a reply email.

### Email Reader Alerts

You can be alerted by email if the Ticketing > Email Reader fails using Monitor > [Alerts - System](#) (page 256) alerts.

### Email Address

Enter the email address you wish to retrieve email messages from periodically. Replies to this email address are in turn processed by the ticketing system and added as notes to the relevant ticket.

### Disable email reader

Check this box to prevent the email reader component from polling a server.

### View Log

Click [View Log](#) to review the polling log for this email reader.

### Turn off independent ticket sequence numbering (use identity value)

For partition 1, single tenant environments only, if checked, ticket numbers match the ticket numbers displayed in outbound emails. If unchecked, these two numbers can be different. These number always match in additional partitions.

## Host Name

The name of the POP3 host service is needed. POP3 is the only email protocol supported. An example is `pop.gmail.com`.

## Port

Provide the port number used by the POP3 service. Typically non-SSL POP3 ports are 110 and SSL POP3 ports are 995.

## Use SSL

Check this box to enable SSL communications with your POP server. Your POP server must support SSL to use this feature. Typically, SSL enabled POP3 servers use port 995.

## Logon

Enter the email account name. Do not include the @ domain name with the account name. For example, if the **Email Address** is `jsmith@acme.com`, then enter `jsmith` as the account name.

## Password

Enter the email account password.

## Check for new emails every <N> minutes

The number of minutes the **Email Reader** should wait before polling the POP3 server for new emails.

## Reject inbound emails containing the following in the subject line

This option only displays for **master role users** (*page 600*). Enter text to ignore inbound emails containing this text *in the subject line*. Matching is case insensitive. *Quotes and wildcard characters such as \* and ? are interpreted literally as part of the string content*. Create multiple filters using multiple lines. Multiple filters act as an OR statement. Surround whole words with spaces on both sides of each word. Example:

```
Undeliverable  
Do not reply
```

This same ignore list can be maintained in the Ticketing > Email Reader page and the Service Desk > Incoming Email and Alarm Settings > General tab. This list can also be maintained manually by editing the `<Kaseya_Installation_Directory>\Kaseya\KServer\ignoreSubject.txt` file.

## Apply

Click **Apply** to begin using the email reader.

## Connect Now

Click **Connect Now** to connect to the POP3 server immediately instead of waiting for the next polling time. This can be used to test your configuration of the email reader.

---

# Email Mapping

## Ticketing > Email Mapping

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Email Mapping** page assigns default values for **new tickets** created using the **Email Reader** (*page 449*). The default values assigned are based on the email address or email domain of the email *sender*.

## Ticketing

Matching can be optionally filtered by the text entered in the email subject line. This information overrides the standard defaults defined using [Edit Fields](#) (page 448).

### Email Address or Domain

The email address or domain *of the sender*. For example: `j.smith@acme.com` or `acme.com`.

### Set map for unassigned emails

If checked, assigns default field values for inbound emails not covered by any other email map.

### Subject Line Filter

Assigns ticket defaults when the *email subject line matches the filter string*. Matching is case insensitive. No wildcard processing is provided. A single `*`, without any other characters in the filter, means let anything through. Boolean statements are not accepted.

### Associate map with

Click the [Select association](#) link to associate new tickets created using this map with a machine ID, machine group, organization, department or staff record.

### Assignee

Enter the name of the VSA user assigned to new tickets created using this email map.

### Fields

Specify the default field values assigned to new tickets created when an email is received by the ticketing system using this map.

### Create

Click [Create](#) to create a new email map using the header values you have previously selected.

### Delete Icon

Click the delete icon  to delete this record.

### Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

## Chapter 12

# Time Tracking

### In This Chapter

Time Tracking Overview	455
Configuring Time Tracking	455
My Timesheets	457
Approve Timesheets	459
Timesheet Summary	460
Application Logging	460
Timesheet History (Summary)	461
Timesheet History (Details)	461
Timers	461
Settings	466
Periods	466
Administrative Tasks	467
Approval Patterns	467

## **Time Tracking**

### **About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

## Time Tracking Overview

**Time Tracking** enables users to record how they use their time, both inside and outside of the Kaseya application.

- **Timesheets** are the main records used to track users' time. Time entries within a timesheet integrate with other functions in the VSA, depending on their work type: administrative tasks, work orders, service desk tickets, or project tasks. You can also export timesheets for billing purposes outside of the VSA.
- **Timers** provide an easy way of creating time entries. Users can start and stop one or more **timers** (page 461) and generate time entries for the elapsed times. Timers don't have to turn off when you log out of the VSA. You can log back in several hours later and apply the elapsed time then, up to a maximum of 24 hours.
- **My Timesheets** - Your own timesheets are accessed using Time Tracking > **My Timesheets** (page 457).
- **Approved Timesheets** - Timesheets are approved using Time Tracking > **Approve Timesheets** (page 459).
- **Time Tracking Reports** - See the **Timesheet Summary** (page 177) and **Timesheet Entries** (page 177) reports in InfoCenter > Reports.

**Note:** See **Time Tracking** (page 453) configuration options.

---

Functions	Description
<b>My Timesheets</b> (page 457)	Tracks your time using timesheets. Timesheets can be saved, submitted for approval or exported to Excel spreadsheet.
<b>Approve Timesheets</b> (page 459)	Approves, rejects or voids submitted timesheets.
<b>Timesheet Summary</b> (page 460)	Provides a summary of the status of all timesheet periods.
<b>Timers</b> (page 461)	Records elapsed time and applies it to timesheets and other work type records.
<b>Periods</b> (page 466)	Creates a series of time periods.
<b>Administrative Tasks</b> (page 467)	Defines tasks representing recurring operational activities, unassociated with specific projects.
<b>Approval Patterns</b> (page 467)	Defines one-step or two-step approvals patterns. Two types of approvers can approve a timesheet:

---

## Configuring Time Tracking

### Configuring Timesheets and Automatic Approvals

- Disable **Use the Timesheet feature for time entry approval** using Time Tracking > **Settings** (page 466).
- Create and activate *a series of time periods* using **Periods** (page 466). A time period must be *active* to display a timesheet for that period in **My Timesheets**.

## Time Tracking

- Activate or close individual time periods using Time Tracking > **Timesheet Summary** (page 460). You can also use this page to review all timesheets by period and by their status: pending, submitted, approved, or voided.
- Link VSA user records to staff records within an organization using System > Orgs/Groups/Depts/Staff > Manage > **Staff** (page 410). This is done automatically when a new VSA user is created.

## Manually Approving Timesheets

To approve timesheets *manually using one or two approvers*, the following configuration steps are required:

- Enable **Use the Timesheet feature for time entry approval** using Time Tracking > **Settings** (page 466).
- Define and *activate* at least one approval pattern using Time Tracking > **Approval Patterns** (page 467).
- Link VSA user records to staff records within an organization using System > Orgs/Groups/Depts/Staff > Manage > **Staff** (page 410). This applies to both VSA users being approved and VSA users acting as approvers. Using this same tab:
  - Link staff records whose timesheets require approval to an activated approval pattern using System > Orgs/Groups/Depts/Staff > Manage > **Staff** (page 410).
  - Ensure the staff record being approved is assigned the supervisor acting as the approver.
  - If the approval pattern specifies two approvers, ensure the supervisor acting as the *first* approver is assigned the supervisor acting as the *second* approver.

**Note:** Approvers can only approve timesheets in their own organization. Approvers can be in different scopes and roles from the users submitting timesheets to them.

- Using this same page you can optionally enable a staff member, by exception, with the ability to approve any timesheet in his or her organization. This ensures all timesheets can be approved in a timely manner, if other approvers are temporarily unavailable.

**Note:** Timesheets are auto-approved if a staff record does not specify an approval pattern and a supervisor.

Once timesheet approvals are configured, submitted timesheets display in the approver's Time Tracking > **Approve Timesheets** (page 459) page after timesheets are submitted to them. The approver can approve, reject or void the submitted timesheet.

## Configuring Timers

- Ensure **Show Session Timer** is enabled by user role, using System > User Roles > **Access Rights** (page 401).
- Enable **Timer Sessions** using Time Tracking > **Settings** (page 466).
  - Check **Show session timers at the header**.
  - Optionally check **Allow multiple session timers running at the same time**.

**Note:** Timers can be used to create time entries even if **Show Timesheets** is disabled.

- Link VSA user records to staff members records within an organization using System > Orgs/Groups/Depts/Staff > Manage > **Staff** (page 410).

**Note:** VSA user logons are typically associated with staff member records in the myOrg (page 594) organization.

---

# My Timesheets

## Time Tracking > My Timesheets

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **TimeSheets** page enables you to track your time using timesheets. Each timesheet represents a different time period. Timesheets can be saved, submitted for **approval** (page 459) or exported to Excel spreadsheet.

Time entries can be created manually, or you can use **timers** (page 461) to record elapsed time and apply that time to your current spreadsheet.

**Note:** Only timesheets for the current date and earlier display in **My Timesheets** (page 457) and **Approve Timesheets** (page 459).

**Note:** See **Time Tracking** (page 453) configuration options.

## Work Types

Work types determine how time entries are integrated with other functions in the VSA. The work type options displayed in your VSA depend on the modules installed.

- **Admin Tasks** - A recurring operational activity not associated with any project.
- **Work Orders** - Only displays if the **Kaseya Billing Service** is installed.
- **Service Desk Tickets** - Only displays if **Kaseya Service Desk 1.3** or later is installed.

## Actions

- **Period** - Selects a timesheet period to display.
- **Add Entry** - Creates a timesheet entry in the displayed timesheet.
  - **Creating an Administrator Task Timesheet Entry** (page 458)
  - **Creating a Customer / Work Order Timesheet Entry** (page 458)
  - **Creating a Service Desk Ticket Timesheet Entry** (page 458)
- **Change Work Type** - Edits a selected entry in the displayed timesheet.
- **Save** - Saves the displayed timesheet.
- **Submit** - Submits a displayed timesheet for approval. Submitted timesheets cannot be edited. Timesheets cannot be submitted before the end of the period.
- **Export to Excel** - Exports an unsubmitted timesheet.

## Columns

This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 18). In addition you can select a column heading to group by.

## Entering Time

For any activity row that already exists, select a cell and enter the number of hours.

## Editing Timesheet Entries - For Admin Tasks Only

Select a cell and click **Change Work Type** to display the **Change Timesheet Entry** window. Enter the following attributes for **Admin Tasks**, a recurring operational activity not associated with any project.

- **Task Name** - Select the task that best describes the time you are recording. Tasks display in the **Ref 1** column on this page.
- **Reference** - Create a filterable, sortable reference to this task in table views and reports. References display in the **Ref 2** column on this page.
- **Billable** - If checked, this time entry is billable.

## Creating an Administrator Task Timesheet Entry

Create an **Admin Task** timesheet entry to track time for **recurring operational activities** (page 467) unassociated with specific projects or with **Service Billing** or with **Service Desk**.

1. Select a timesheet using Time Tracking > **My Timesheets**.
2. Add a new entry to the timesheet by clicking **Add Entry**. The **New Timesheet Entry** dialog displays.
3. Enter a date and time for the timesheet entry.
4. Select the **Admin Task** work type option.
5. Select the **Task Name** that best describes the time you are recording. Tasks display in the **Ref 1** column of the timesheet.
6. **Reference** - Enter a free-form reference. Example: Customer PO number. References display in the **Ref 2** column of the timesheet.
7. Optionally add a **Note**.
8. Click **Save** to close this dialog. The new entry displays in the timesheet.
9. Click **Save** to save your changes to the timesheet.

## Creating a Customer / Work Order Timesheet Entry

Create a **Customer / Work Order** timesheet entry to direct the time entered to **Service Billing**. **Service Billing** time entries can be billed to the customer.

1. Select a timesheet using Time Tracking > **My Timesheets**.
2. Add a new entry to the timesheet by clicking **Add Entry**. The **New Timesheet Entry** dialog displays.
3. Enter a date and time for the timesheet entry.
4. Select the **Customer / Work Order** work type option.
5. Select a **Customer**. The customer displays in the **Ref 1** column of the timesheet.
6. Select the **Work Order**. The work order displays in the **Ref 2** column of the timesheet.
7. Select the **Task Name**. The **Task Name** is the work order item you want to enter entry detail for.
8. Optionally add a **Note**.
9. Optionally check the **Show Note on Invoice** checkbox.
10. Classify this entry by **Activity Type**. The activity type displays in the **Activity** column of the timesheet.
11. Ensure the **Billable** checkbox is checked if you want to bill for this activity.
12. Click **Save** to close this dialog. The new entry displays in the timesheet.
13. Click **Save** to save your changes to the timesheet.
14. The entry you created will be eligible for billing once the timesheet is submitted and approved.

## Creating a Service Desk Ticket Timesheet Entry

Create a **Service Desk Ticket** timesheet entry to add the time to the entire **Service Desk** ticket. You can optionally link the ticket to **Service Billing** records or to a task, if either one of these features is enabled. Time entered displays as a note in the ticket.

1. Select a timesheet using Time Tracking > **My Timesheets**.
2. Add a new entry to the timesheet by clicking **Add Entry**. The **New Timesheet Entry** dialog displays.
3. Enter a date and time for the timesheet entry.
4. Select the **Service Desk Ticket work type** (page 600) option.
5. Select the **Service Desk** definition.
6. Optionally select a **Status Filter** to limit the list of tickets displayed in the **Ticket** drop-down list.display.
7. Select either:

- [Show All Tickets](#)
  - [Show My Tickets](#)
8. Select a **Ticket**.
  9. The following fields display only if the **Service Billing** is installed and integrated with **Service Desk**. See [Creating Billing Entries using Service Desk](#).
    - **Work Order** - Display only. Displays only if a work order is associated with the ticket on the General tab of the ticket editor.
    - **Work Order Item** - The work order line to associate with the hours worked. Displays only if a work order is associated with the ticket on the General tab of the ticket editor.
    - **Activity Type** - Labor entries are grouped by **activity type** to analyze the cost and revenue of labor. The classification of activity types typically reflects the accounting requirements of a company. Labor entries are classified by both activity type and resource type. Not editable if a detailed work order is selected.
    - **Resource Type** - A **resource type** specifies a *skill*, *material* or *cost* and sets a default rate for a billable labor item or entry. Typically a resource type represents a skill performed by a staff member. A billing rate and standard cost is defined for each *skill* required to perform the service. The rate can be overridden when selected. Because the labor performed to deliver a service sometimes requires incidental charges for materials and costs, resource types can also be classified as either *material* or *cost*. For example, extra cabling or overnight shipping might be included as additional, billable labor entries, because they are required to deliver the service of installing a server. The classification of resource types typically reflects the production requirements of a company. Labor entries are classified by both resource type and by activity type. Not editable if a detailed work order is selected.
    - **Rate** - The default billing rate for the selected resource type. Display only.
    - **Override Rate** - A manually entered rate that overrides the default billing rate for a selected resource type. Does not display if a detailed work order is selected.
    - **Show Note on Invoice** - If checked, the note is displayed on the printed invoice.
  10. Select a **Task**. This field only displays if Tasks are enabled for the service desk.
  11. Optionally add a **Note**.
  12. Optionally make the note a **Hidden Note** in the ticket.
  13. **Billable** - If checked, the entry is billable. If **Service Billing** is not installed, the **Billable** checkbox is for reference purposes only. If **Service Billing** is installed the entry is forwarded to **Service Billing**. If timesheets require approval, the timesheet containing this entry must be approved before the entry is forwarded to **Service Billing**.
  14. Click **Save** to close this dialog. The new entry displays in the timesheet.
  15. Click **Save** to save your changes to the timesheet.

---

## Approve Timesheets

### Time Tracking > Approve Timesheets

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The [Approve Timesheets](#) page approves timesheets submitted by VSA users to them using [My Timesheets](#) (page 457). Approvers can approve, reject or void a timesheet. Clicking the hyperlink underneath a name in the **Staff** column displays the details of that timesheet.

**Note:** Only timesheets for the current date and earlier display in [My Timesheets](#) (page 457) and [Approve Timesheets](#) (page 459).

**Note:** See [Time Tracking](#) (page 453) configuration options.

### Actions

- **Approve** - Approves selected timesheets.

**Note:** If timesheets require approval, a time entry is not forwarded to **Service Billing** until the timesheet is approved.

- **Reject** - Rejects selected timesheets, returning them for correction to their timesheet submitters in **My Timesheets**.
- **Void** - Prevents selected timesheets and their time entries from being processed any further throughout the system.

---

## Timesheet Summary

### Time Tracking > Timesheet Summary

- This page applies to the following products: **On Premises**, **Kaseya Advanced**, **Kaseya Essentials**, **IT Center**

The **Timesheet Summary** page provides a summary of the status of all timesheet periods. Activating a timesheet period enables all VSA users to access that timesheet period in **Time Tracking > My Timesheets** (page 457) and **Time Tracking > Approve Timesheets** (page 459).

### Actions

- **Close Period** - Close a selected timesheet period, preventing further changes to timesheets in that period.
- **Activate Period** - Activate a selected timesheet period, enabling changes to timesheets in that period.

### Column Headings

Clicking any number in one of the cells of the table grid displays a secondary window listing the status of each timesheet in that state and time period.

- **Period** - The date range of a timesheet period.
- **Status** - Indicates the timesheet period is either **Active** or **Closed**.
- **Pending** - The number of timesheets being updated by users in this period, before being submitted.
- **Submitted** - The number of timesheets submitted in this period, before being approved.
- **Approved** - The number of timesheets approved in this period.
- **Voided** - The number of timesheets voided in this period.

---

## Application Logging

### Time Tracking > Application Logging

- This page applies to the following products: **On Premises**, **Kaseya Advanced**, **Kaseya Essentials**, **IT Center**

The **Application Logging** page displays a log of **Time Tracking** module activity by:

- **Event ID**
- **Event Name**
- **Message**
- **Admin**
- **Event Date**

This table supports **selectable columns**, **column sorting**, **column filtering** and **flexible columns widths** (page 18).

---

## Timesheet History (Summary)

### Time Tracking > Timesheet History (Summary)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Timesheet History (Summary)** page provides summary of all time entries in a tabular view. The table displays a single row for each unique combination of **User**, **Date**, **Work Type**, **Ref 1** and **Ref 2**.

Columns of data for each time sheet entry include:

- **Status** - New, Approved, Submitted, Void
- **User** - The staff record name.
- **Work Type** - Admin Task, Work Order, Service Desk Ticket, Project Task.
- **Ref 1** - The name of the task.
- **Ref 2** - A free-form reference. Example: Customer PO number.
- **Activity** - A description of the time activity you are recording.
- **Billable** - If checked, this time entry is billable.
- **Time Period** - The time period of the time entry.
- **Date** - The date of the time entry
- **Hours** - The total number of hours entered for duration of the time entry.

This table supports **selectable columns**, **column sorting**, **column filtering and flexible columns widths** (page 18).

---

## Timesheet History (Details)

### Time Tracking > Timesheet History (Details)

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Timesheet History (Details)** page provides all time entries in a tabular view. Columns of data for each time sheet entry include:

- **Status** - New, Approved, Submitted, Void
- **User** - The staff record name.
- **Work Type** - Admin Task, Work Order, Service Desk Ticket, Project Task.
- **Ref 1** - The name of the task.
- **Ref 2** - A free-form reference. Example: Customer PO number.
- **Activity** - A description of the time activity you are recording.
- **Billable** - If checked, this time entry is billable.
- **Note** - Additional text, if appropriate, describing this time entry.
- **Time Period** - The time period of the time entry.
- **Date** - The date of the time entry
- **Hours** - The duration of the time entry.

This table supports **selectable columns**, **column sorting**, **column filtering and flexible columns widths** (page 18).

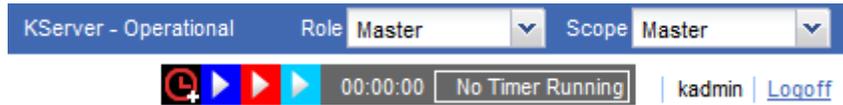
---

## Timers

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

## Time Tracking

A timer control panel displays in the upper right hand corner of the VSA, just below the Role/Scope Selector.



Timers enable you to record the time you take to perform a task. Then you can add the elapsed time as a timesheet entry. You can run multiple timers concurrently. The entries you create display in the Time Tracking > [My Timesheets](#) (page 457) page.

Timers don't have to turn off when you log out of the VSA. You can log back in several hours later and apply the elapsed time then.

**Note:** See [Time Tracking](#) (page 453) configuration options.

### Adding a Timer

Timer entries can be applied using the following [work types](#) (page 600):

- [Creating an Administrator Task Timer Entry](#) (page 463)
- [Creating a Customer / Work Order Timer Entry](#) (page 463)
- [Creating a Service Desk Ticket Timer Entry](#) (page 464)

### Working with Timers

Once a timer is added, a selected timer in the timer bar displays the color and name of the timer. When a timer is running, the **Pause**  button displays. When a timer stops, the **Play**  button displays. You can run multiple timers if this is enabled in Time Tracking > [Settings](#) (page 466).

### Timer Action Buttons

Hovering the mouse cursor over a specific timer activates the action buttons for that timer.



- The timer's color, label and elapsed time are displayed.
- Both the label field and the color field are editable.
- Click the Checkmark  icon to display the [Apply Time](#) window. You can edit your time entry, including the elapsed time, and either:
  - [Apply and Remove](#) - Apply your time entry to your timesheet and remove the timer.
  - [Apply and Reset](#) - Apply your time entry to your timesheet and reset the timer to 0.
- Ctrl+click the Checkmark  icon to apply your elapsed time to your timesheet immediately, in the cell for today's date. You can edit the time entry later using Time Tracking > [My Timesheets](#) (page 457).
- The Reset Timer  icon resets the elapsed time back to 0.
- The Remove Timer  icon removes the timer without applying elapsed time to your spreadsheet.

### Add Time Action Buttons

Hovering the mouse cursor over the [Add Timer](#) icon timer activates the action buttons for that icon.



- Click [New Timer](#) to create a new time.
- Click [Pause All](#) to stop all timers at once.

- Click **Delete All** to remove all timers.

## Creating an Administrator Task Timer Entry

Create an **Admin Task** timer entry to track time for **recurring operational activities** (page 467) unassociated with specific projects or with **Service Billing** or with **Service Desk**.

1. Click the add timer  icon to add a new timer. Timers are located in the upper right hand corner of the VSA window. The **New Timer** dialog displays. Enter or select values for the following fields.
2. Select a unique **Timer Color**. You can define multiple timers concurrently so it helps to assigned them different colors.
3. Enter a **Label** for your timer. The label displays whenever the timer icon is selected and added as a note to any time entry you create from the timer. If blank, the timer is labeled by the work type you select.
4. If **Start of Save** is checked, the time starts running as soon as you save this dialog.
5. Select the **Admin Task** work type option.
6. Select the **Task Name** that best describes the time you are recording. Tasks display in the **Ref 1** column of a timesheet.
7. **Reference** - Enter a free-form reference. Example: Customer PO number. References display in the **Ref 2** column of a timesheet.
8. Optionally add a **Note**.
9. Click **Save** to close this dialog. The new timer clocks begins recording the time for this activity.
10. Complete the activity being timed by this timer.
11. Click the Checkmark  icon. You can edit your time entry, including the elapsed time, and either:
  - **Apply and Remove** - Apply your time entry to your timesheet and remove the timer.
  - **Apply and Reset** - Apply your time entry to your timesheet and reset the timer to 0.
12. The entry you created will be eligible for billing once the timesheet is submitted and approved.

## Creating a Customer / Work Order Timer Entry

Create a **Customer / Work Order** timer entry to direct the time entered to **Service Billing**. **Service Billing** time entries can be billed to the customer.

1. Click the add timer  icon to add a new timer. Timers are located in the upper right hand corner of the VSA window. The **New Timer** dialog displays. Enter or select values for the following fields.
2. Select a unique **Timer Color**. You can define multiple timers concurrently so it helps to assigned them different colors.
3. Enter a **Label** for your timer. The label displays whenever the timer icon is selected and added as a note to any time entry you create from the timer. If blank, the timer is labeled by the work type you select.
4. If **Start of Save** is checked, the time starts running as soon as you save this dialog.
5. Select the **Customer / Work Order** work type option.
6. Select a **Customer**, **Work Order** and **Task Name**. The **Task Name** is the work order item you want to enter entry detail for.
7. Optionally add a **Note**.
8. Optionally check the **Show Note on Invoice** checkbox.
9. Classify this entry by **Activity Type**.
10. Ensure the **Billable** checkbox is checked if you want to bill for this activity.
11. Click **Save** to close this dialog. The new timer clocks begins recording the time for this activity.

## Time Tracking

12. Complete the activity being timed by this timer.
13. Click the Checkmark ✓ icon to display the **Apply Time** window. You can edit your time entry, including the elapsed time, and either:
  - **Apply and Remove** - Apply your time entry to your timesheet and remove the timer.
  - **Apply and Reset** - Apply your time entry to your timesheet and reset the timer to 0.
14. The entry you created will be eligible for billing once the timesheet is submitted and approved.

## Creating a Service Desk Ticket and Service Billing Timer

### Entry

Create a **Service Desk Ticket** timer entry to add the time to the entire **Service Desk** ticket. You can optionally link the ticket to **Service Billing** records or to a task, if either one of these features is enabled. Time entered displays as a note in the ticket.

1. Click the add timer  icon to add a new timer. Timers are located in the upper right hand corner of the VSA window. The **New Timer** dialog displays. Enter or select values for the following fields.
2. Select a unique **Timer Color**. You can define multiple timers concurrently so it helps to assign them different colors.
3. Enter a **Label** for your timer. The label displays whenever the timer icon is selected and added as a note to any time entry you create from the timer. If blank, the timer is labeled by the work type you select.
4. If **Start of Save** is checked, the time starts running as soon as you save this dialog.
5. Select the **Service Desk Ticket work type** (*page 600*) option.
6. Select the **Service Desk** definition.
7. Optionally select a **Status Filter** to limit the list of tickets displayed in the **Ticket** drop-down list.
8. Select either:
  - **Show All Tickets**
  - **Show My Tickets**
9. Select a **Ticket**.
10. The following fields only display if a service desk is integrated with **Service Billing**. See **Creating Billing Entries using Service Desk**.
  - **Work Order** - Display only. Displays only if a work order is associated with the ticket on the General tab of the ticket editor.
  - **Work Order Item** - The work order line to associate with the hours worked. Displays only if a work order is associated with the ticket on the General tab of the ticket editor.
  - **Activity Type** - Labor entries are grouped by **activity type** to analyze the cost and revenue of labor. The classification of activity types typically reflects the accounting requirements of a company. Labor entries are classified by both activity type and resource type. Not editable if a detailed work order is selected.
  - **Resource Type** - A **resource type** specifies a *skill*, *material* or *cost* and sets a default rate for a billable labor item or entry. Typically a resource type represents a skill performed by a staff member. A billing rate and standard cost is defined for each *skill* required to perform the service. The rate can be overridden when selected. Because the labor performed to deliver a service sometimes requires incidental charges for materials and costs, resource types can also be classified as either *material* or *cost*. For example, extra cabling or overnight shipping might be included as additional, billable labor entries, because they are required to deliver the service of installing a server. The classification of resource types typically reflects the production requirements of a company. Labor entries are classified by both resource type and by activity type. Not editable if a detailed work order is selected.
  - **Rate** - The default billing rate for the selected resource type. Display only.

- **Override Rate** - A manually entered rate that overrides the default billing rate for a selected resource type. Does not display if a detailed work order is selected.
  - **Show Note on Invoice** - If checked, the note is displayed on the printed invoice.
11. Select a **Task**. This field only displays if Tasks are enabled for the service desk.
  12. Optionally add a **Note**.
  13. Optionally make the note a **Hidden Note** in the ticket.
  14. **Billable** - If checked, the entry is billable. If **Service Billing** is not installed, the **Billable** checkbox is for reference purposes only. If **Service Billing** is installed the entry is forwarded to **Service Billing**. If timesheets require approval, the timesheet containing this entry must be approved before the entry is forwarded to **Service Billing**.
  15. Click **Save** to close this dialog. The new timer clocks begins recording the time for this activity.
  16. Complete the activity being timed by this timer.
  17. Click the Checkmark ✓ icon to display the **Apply Time** window. You can edit your time entry, including the elapsed time, and either:
    - **Apply and Remove** - Apply your time entry to your timesheet and remove the timer.
    - **Apply and Reset** - Apply your time entry to your timesheet and reset the timer to 0.

## Creating a Service Desk Ticket or Ticket/Task Timer Entry

Create a **Service Desk Ticket** timer entry to add the time to either the entire **Service Desk** ticket or to a task within a **Service Desk** ticket. Time entered displays as a note in the ticket.

1. Click the add timer  icon to add a new timer. Timers are located in the upper right hand corner of the VSA window. The **New Timer** dialog displays. Enter or select values for the following fields.
2. Select a unique **Timer Color**. You can define multiple timers concurrently so it helps to assigned them different colors.
3. Enter a **Label** for your timer. The label displays whenever the timer icon is selected and added as a note to any time entry you create from the timer. If blank, the timer is labeled by the work type you select.
4. If **Start of Save** is checked, the time starts running as soon as you save this dialog.
5. Select the **Service Desk Ticket** work type option.
6. Select the **Service Desk** definition.
7. Optionally select a **Status Filter** to limit the list of tickets displayed in the **Ticket** drop-down list.
8. Select either:
  - **Show All Tickets**
  - **Show My Tickets**
9. Select a **Ticket**.
10. Select a **Task**. This field only displays if the Task Functionality feature is enabled in **Service Desk**.
11. Optionally add a **Note**.
12. Optionally make the note a **Hidden Note** in the ticket.
13. **Billable** - If checked, the entry is billable. If **Service Billing** is not installed, the **Billable** checkbox is for reference purposes only. If **Service Billing** is installed the entry is forwarded to **Service Billing**. If timesheets require approval, the timesheet containing this entry must be approved before the entry is forwarded to **Service Billing**.
14. Click **Save** to close this dialog. The new timer clocks begins recording the time for this activity.
15. Complete the activity being timed by this timer.
16. Click the Checkmark ✓ icon to display the **Apply Time** window. You can edit your time entry, including the elapsed time, and either:
  - **Apply and Remove** - Apply your time entry to your timesheet and remove the timer.
  - **Apply and Reset** - Apply your time entry to your timesheet and reset the timer to 0.

## Time Tracking

- **Apply and Remove** - Apply your time entry to your timesheet and remove the timer.
- **Apply and Reset** - Apply your time entry to your timesheet and reset the timer to 0.

---

# Settings

## Time Tracking > Settings

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

### Time Tracking

- **Use the Timesheet feature for time entry approval** - If checked, timesheets are manually approved using Time Tracking > **Approve Timesheets** (page 459). If blank, timesheets are automatically approved.

**Note:** Timesheets are also auto-approved if a staff record does not specify an approval pattern and a supervisor.

**Note:** See Time Tracking (page 453) configuration options.

### Billing

- **Submit Time Entry Data to Service Billing** - Only displays if Service Billing is installed. If checked, time entries created using **My Timesheets** (page 457) or **timers** (page 461) can be passed to Service Billing and billed. If timesheets require approval, a time entry is not forwarded to **Service Billing** until the timesheet is approved.

### Session Timers

- **Show session timers at the header** - If checked, timers displays in the header of the VSA.
- **Allow multiple session timers running at the same time** - If **Show session timers** is checked, enable or disable running multiple sessions at the same time.

**Note:** See Time Tracking (page 453) configuration options.

---

# Periods

## Time Tracking > Periods

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

The **Periods** page defines a *series of time periods*. Each **Periods** record specifies a start date, duration and standard calendar unit of time—weekly or monthly, for example. These values are used to create a series of time periods.

Only one **Periods** record can be activated at any one time. Activating a **Periods** record enables time entries to be applied to its time periods. All generated time periods are active by default. You can use Time Tracking > **Timesheet Summary** (page 460) to close a time period.

If **timesheets** and **timers** are enabled using Time Tracking > **Settings** (page 466), then these features can be used to create and maintain time entries for an active time period.

Generally, this function only needs to be run once a year, to create one or two more years of timesheets.

**Note:** Only timesheets for the current date and earlier display in **My Timesheets** (page 457) and **Approve Timesheets** (page 459).

**Note:** See Time Tracking (page 453) configuration options.

## Actions

- **New** - Create a periods record.
- **Edit** - Edit a selected periods record.
- **Activate** - Activate a selected periods record.
- **Deactivate** - Deactivate a selected periods record.
- **View Periods** - View the time periods of a selected periods record.

## Adding or Editing a Time Period

- **Name** - Enter a name for the periods record.
- **Schedule** - Enter a calendar period.
- **Purpose** - *Billing or Timesheet*. Reference only.
- **Starting Date** - The start date to begin generating time periods.

**Note:** The start date also determines the *first day of the week* when timesheets are displayed.

- **Creation Period** - The length of time to create time periods for.
- **No of hours per period** - The typical number of work hours associated with each time period. Used for comparison with the actual hours entered.

---

# Administrative Tasks

## Time Tracking > Administrative Types

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center*

The **Administrative Tasks** page defines tasks that represent recurring operational activities, unassociated with specific projects. *Vacation, Meetings, and Travel* are typical examples. This table includes a set of predefined (*System*) administrative tasks.

When creating a time entry using a **Timer** (*page 461*) you're given the option of classifying the elapsed time as an administrative task. The **Work Type** (*page 600*) column in **Time Tracking > My Timesheets** (*page 457*) identifies these time entries as *Admin Task*.

## Actions

- **New** - Create a new task.
- **Edit** - Edit an existing task.

## Adding or Editing an Administrative Task

- **Name** - Enter a name for the task.
- **Desc** - Enter a description for the task.
- **Enabled** - If checked, the task can be added to a timesheet.
- **Automatically Added to Timesheets** - If checked, the task is automatically added to a timesheet.

---

# Approval Patterns

## Time Tracking > Approval Patterns

- This page applies to the following products: *On Premises, Kaseya Advanced, Kaseya Essentials, IT Center*

The **Approval Patterns** page defines one-step or two-step approvals patterns. Two types of approvers can approve a timesheet:

- The **supervisor** of another staff member—as specified using the **Supervisor** drop-down list in *System > Orgs/Groups/Depts/Staff > Manage > Staff* (*page 410*).

## Time Tracking

- A **manager**, which is the *supervisor of a supervisor*.

Approval patterns can be created that require approval from a Supervisor, a Manager, or either. For example:

- Supervisor only
- Manager only
- Supervisor or Manager - A single approval by either one is required to approve a timesheet.

**Note:** The staff records of both approvers and those being approved must be associated with their own VSA user logons.

**Note:** See Time Tracking (page 453) configuration options.

## Actions

- **New** - Create a new approval pattern.
- **Edit** - Edit an existing approval pattern.
- **Activate** - Activate an approval pattern.
- **Deactivate** - Deactivate an approval pattern. Deactivating an approval pattern clears that approval pattern from all staff records that are using it. All subsequent timesheets submitted by those staff members are auto-approved until a new approval pattern is assigned to their staff records.

## Adding or Editing an Approval Pattern

- **Pattern Name** - Enter the name of the approval pattern.
- **First Approver** - Supervisor or Manager.
- **Second Approver** - Supervisor or Manager or leave blank.

## Chapter 13

# Database Views

### In This Chapter

Database Views	472
Excel Usage	472
Crystal Reporting Usage	473
Views Provided	477
fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy	478
fnOSCounts	479
vAddRemoveList	480
vAdminNotesLog	480
vAgentConfiguration	480
vAgentLabel	482
vAlertLog	482
vBackupLog	483
vBaseApplicationInfo / vCurrApplicationInfo	484
vBaseCpuInfo / vCurrCpuInfo	485
vBaseDiskInfo / vCurrDiskInfo	485
vBaseDriveManufacturer / vCurrDriveManufacturer	486
vBasePciInfo / vCurrPciInfo	486
vBasePrinterInfo / vCurrPrinterInfo	487
vCollectionMember	487
vConfigLog	488
vkadComputers	488
vkadUsers	489
vLicenseInfo	489
vMachine	490
vMonitorAlarmAlert	492
vMonitorAlarmCounter	493
vMonitorAlarmProcess	494
vMonitorAlarmService	494
vMonitorAlarmSNMP	495
vMonitorAlarmSystemCheck	496
vNetStatsLog	497

## Database Views

vNtEventLog	497
vOnBoardDeviceInfo	498
vPatchApprovalStatus	498
vPatchConfiguration	499
vPatchPolicy	501
vPatchPolicyMember	502
vPatchStatus	502
vPortInfo	504
vScriptLog	505
vScriptStatus	505
vSystemInfo	506
vSystemInfoManual	507
vTicketField	507
vTicketNote	508
vTicketSummary	508
vUptimeHistory	509
vvProAssetDetails	509

**About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

## Database Views

### System > Database Views

The system exposes a set of **database views and database functions** (page 477) allowing clients to directly access data within the Kaseya repository. The database functions can be thought of as parameterized views. These views can be used to bring data into a spreadsheet for analysis or to prepare reports. This document describes the views and functions and gives two example applications, **Crystal Reporting** (page 473) and **Microsoft Excel** (page 472). Kaseya does not present itself as an expert in how to use Excel or Crystal. These examples are to assist in the basics of getting started. For third party product training or other questions please contact the third party tool vendor. Finally, an appendix is provided with a field-by-field description of the contents of the views and functions.

The views provided can be broken into **four groups of database views** (page 477).

- The first group provides information on all the **machines** being monitored.
- The second group provides information about the **activity and current status** of key parts of the system.
- The third group provides information on the **ticketing** system.
- The fourth group provides information on the **monitoring** alarms.

### Accessing the Database Views

The database views are installed or updated whenever the **Reapply Schema** action is taken. A single database user ID, `KaseyaViews` is provided to access these views.

1. For security purposes, you must first create or change the password for the `KaseyaViews` user ID by entering the password in the System > **Database Views** page.
2. From that point forward, you can use external applications, such as Crystal Reports or Excel, to access the database views directly, using the `KaseyaViews` user ID and the password you have entered.

**Note:** If you have a problem connecting to SQL Server 2005 using the `KaseyaViews` user ID, see Kaseya KB article 307669 (<http://help.kaseya.com/WebHelp/KB-Article.asp?307669>).

---

## Excel Usage

### Creating a Data Source in Windows

Microsoft Excel can access the views by setting up a data source. A data source is a core definition within Microsoft. Most Microsoft products have facilities to access data through a data source definition. Selecting the Settings option from the Start button allows the creation a data source. From the Settings option select the Control Panel. From the Control Panel next select Administrative Tools. From this menu a data source can be created.

The data source should be set up as a System DSN. From this dialog, create a source using the SQL Server driver. The set-up will require the name of the database server (usually the ComputerName), the user id (`KaseyaViews`) and password, and the database schema name (`ksubscribers`).

### Selecting the Data Source in Excel

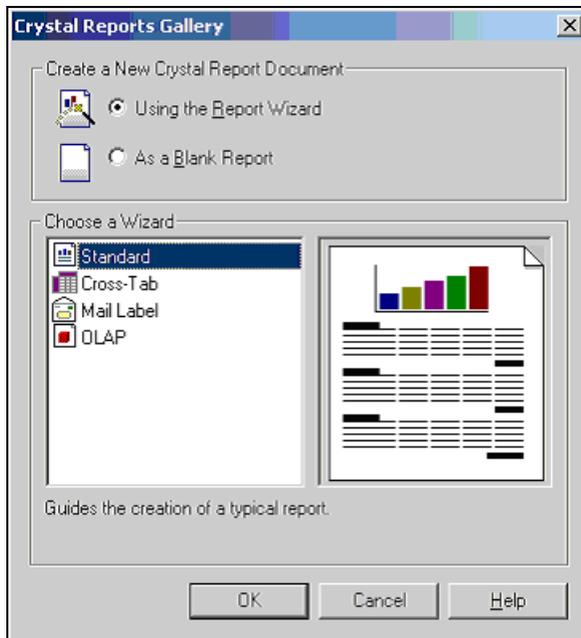
Once a data source is created it can be referenced by Excel. Open a blank spreadsheet and select the **Data > Get External Data > New Database Query...** option. The user is prompted for the credentials to the database. Once this completes a view can be selected. A SQL query can be constructed to bring information directly into Excel at this point.

---

## Crystal Reporting Usage

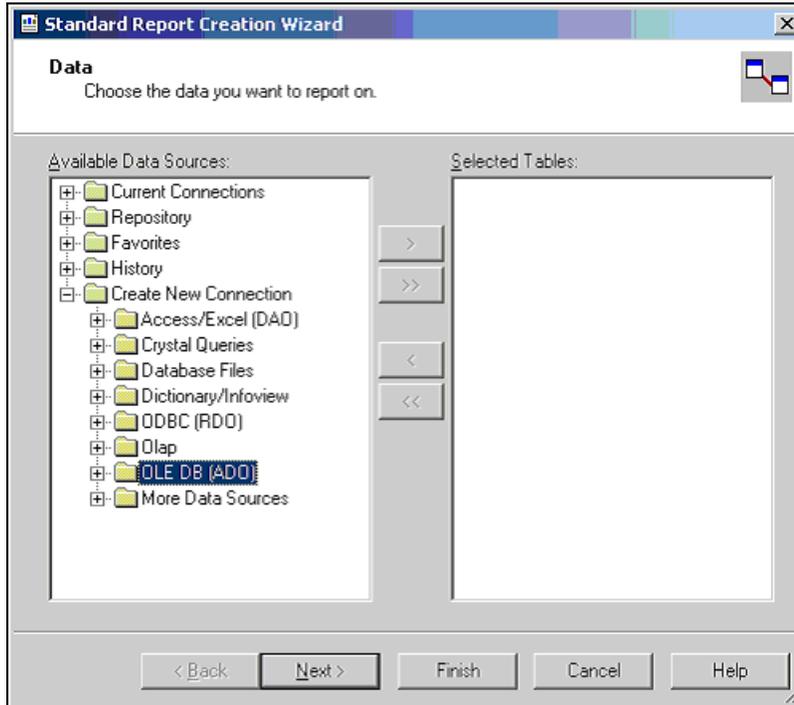
Crystal Reporting can be used to create client specified reports. Crystal 9 and 10 can be used to produce various output formats include PDF, Word and Excel. To set up a report the Crystal Report Wizard can be used. This process begins with the following dialog.

1. The client picks a report format. For this example standard will be used.

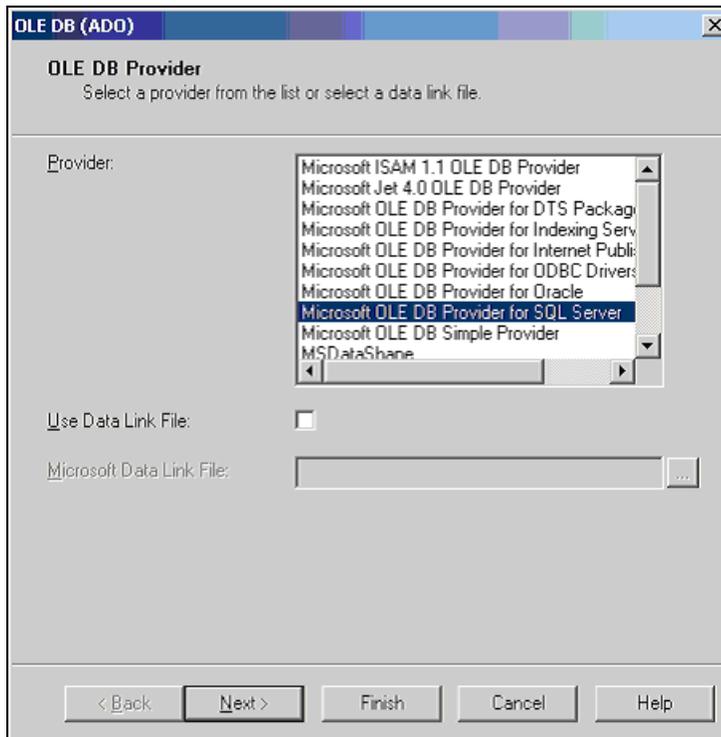


## Database Views

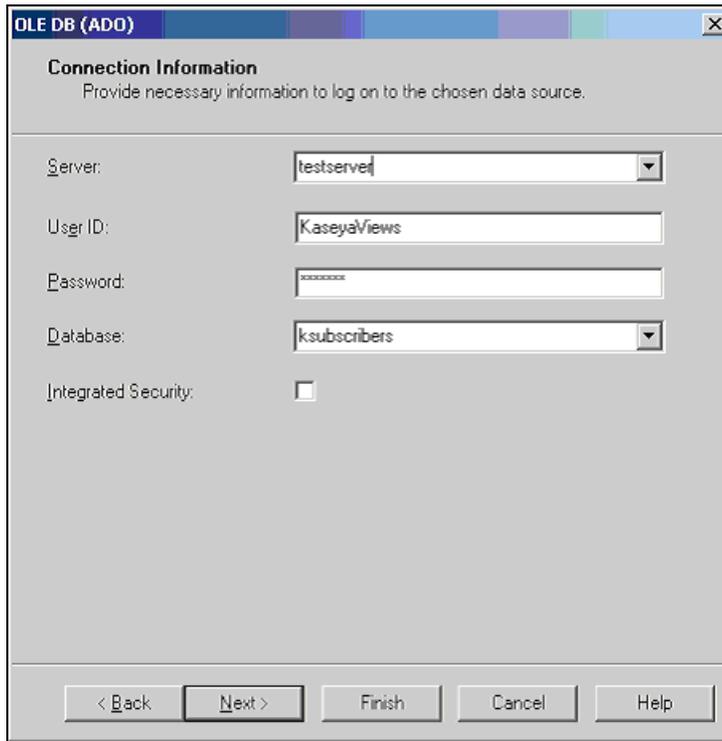
2. Next the data source is selected. This begins by picking an access method. ADO should be selected.



3. Once ADO is selected the SQL Server driver can be selected. This is the correct selection to access the Kaseya database.

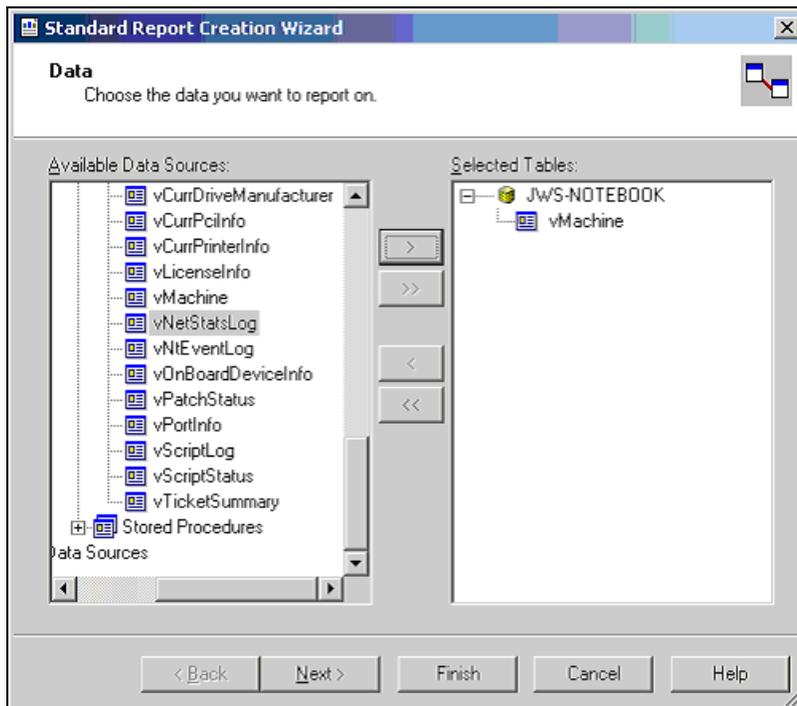


4. The next step is providing the credential to make connection to the database. As shown in this dialog, the Server, User Id, Password, and Database must be provided.



The image shows a dialog box titled "OLE DB (ADO)" with a subtitle "Connection Information". Below the subtitle is the instruction "Provide necessary information to log on to the chosen data source." The dialog contains four input fields: "Server:" with a dropdown menu showing "testserver"; "User ID:" with a text box containing "KaseyaViews"; "Password:" with a text box containing "\*\*\*\*\*"; and "Database:" with a dropdown menu showing "ksubscribers". There is also an "Integrated Security:" checkbox which is unchecked. At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

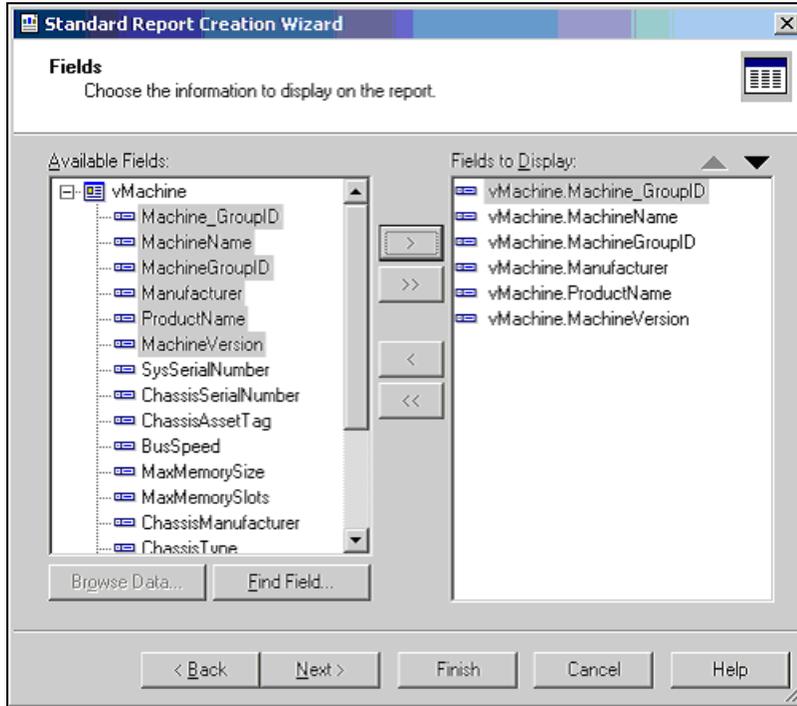
5. Once the credentials are provide all the available views are displayed. Pick one or more for the report desired.



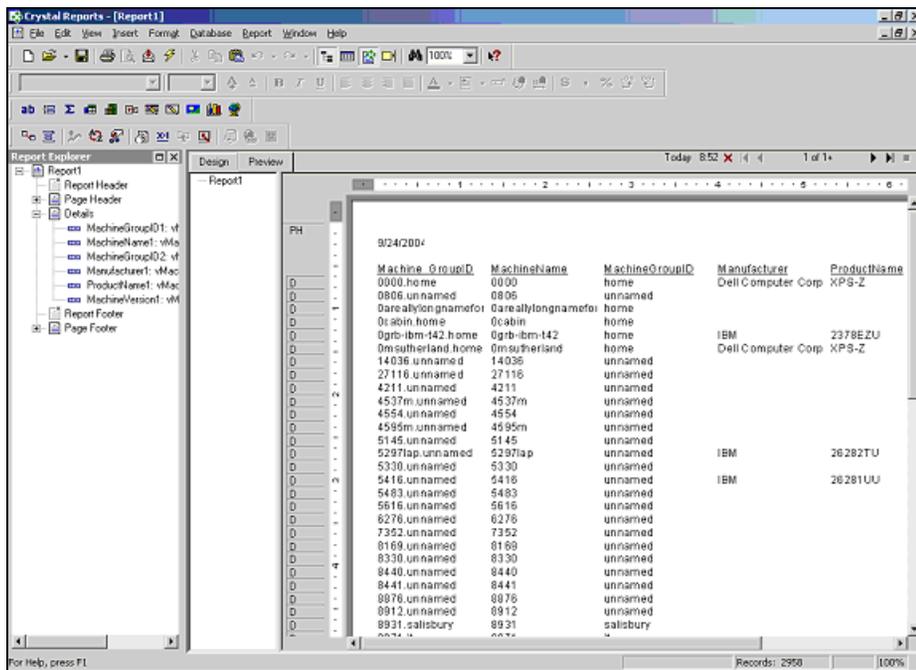
The image shows a dialog box titled "Standard Report Creation Wizard" with a subtitle "Data" and the instruction "Choose the data you want to report on." The dialog is split into two main sections. On the left, under "Available Data Sources:", there is a list of views including vCurrDriveManufacturer, vCurrPcInfo, vCurrPrinterInfo, vLicenseInfo, vMachine, vNetStatsLog, vNIEventLog, vOnBoardDeviceInfo, vPatchStatus, vPortInfo, vScriptLog, vScriptStatus, vTicketSummary, and Stored Procedures. On the right, under "Selected Tables:", there is a tree view showing "JWS-NOTEBOOK" with a sub-item "vMachine". Between the two sections are four arrow buttons: ">", ">>", "<<", and "<". At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

## Database Views

- After a view is selected the columns to be included can then be selected. Crystal provides a variety of ways to format this data. This document does not attempt to describe these options. The Crystal documentation should be reviewed for this information.



- The resulting report can be printed or emailed to the appropriate consumers of the report. The format of the report can be designated. This facility can be used to produce a PDF or a variety of other formats.



# Views Provided

<b>Machines Group</b>	
<a href="#">vAddRemoveList</a> (page 480)	Add/remove application list returned by the latest audit.
<a href="#">vBaseApplicationInfo</a> (page 484)	The baseline list of applications on a client desktop machine.
<a href="#">vBaseCpulInfo</a> (page 485)	The baseline list of the CPUs in a client desktop machine.
<a href="#">vBaseDiskInfo</a> (page 485)	The baseline list of the disks in a client desktop machine.
<a href="#">vBaseDriveManufacturer</a> (page 486)	The baseline list of the manufacturers of the disks in a client desktop machine.
<a href="#">vBasePciInfo</a> (page 486)	The baseline list of the PCI cards in a client desktop machine.
<a href="#">vBasePrinterInfo</a> (page 487)	The baseline list of printers in a client desktop machine.
<a href="#">vCollectionMember</a> (page 487)	List the collections each machine ID belongs to (if any)
<a href="#">vCurrApplicationInfo</a> (page 484)	The current list of applications on a client desktop machine.
<a href="#">vCurrCpulInfo</a> (page 485)	The current list of the CPUs in a client desktop machine.
<a href="#">vCurrDiskInfo</a> (page 485)	The current list of the disks in a client desktop machine.
<a href="#">vCurrDriveManufacturer</a> (page 486)	The current list of the manufacturers of the disks in a client desktop machine.
<a href="#">vCurrPciInfo</a> (page 486)	The current list of the PCI cards in a client desktop machine.
<a href="#">vCurrPrinterInfo</a> (page 487)	The current list of printers in a client desktop machine.
<a href="#">vkadComputers</a> (page 488)	The current list of active directory harvested computers.
<a href="#">vkadUsers</a> (page 489)	The current list of active directory harvested users.
<a href="#">vLicenseInfo</a> (page 489)	The licenses of applications on this machine.
<a href="#">vMachine</a> (page 490)	The information known about each client desktop machine.
<a href="#">vOnBoardDeviceInfo</a> (page 498)	The current list of on board devices in a client desktop machine.
<a href="#">vPortInf</a> (page 504)	The current list of ports in a client desktop machine.
<a href="#">vSystemInfo</a> (page 506)	Data collected by the Audit > <a href="#">System Info</a> (page 140) function.
<a href="#">vSystemInfoManual</a> (page 507)	Custom fields and values added to the SystemInfo function.
<a href="#">vUptimeHistory</a> (page 509)	Data collected for the uptime history report. Use in conjunction with the getMachUptime web service.
<a href="#">vvProAssetDetails</a> (page 509)	Lists information about a vPro enabled machine, including manufacturing details about the motherboard.
<b>Activity / Status Group</b>	
<a href="#">fnMissingPatchCounts_UsePolicy</a> (page 478)	Returns the number of patches, using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the executive summary reports and the View Dashboard page under the Home tab. Only one row is returned.
<a href="#">fnMissingPatchCounts_NoPolicy</a> (page 478)	Returns the number of patches, without using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the View Dashboard page under the Home tab. Only one row is returned.
<a href="#">fnOSCounts</a> (page 479)	Returns the types of operating systems and the counts for each for the specified machine group. Tabular data as seen in the OS pie charts in the executive summary reports and the View Dashboard page under the Home tab. Returns one row for each OSType.
<a href="#">vAdminNotesLog</a> (page 480)	Notes each admin enters manually for a machine or group of machines.

## Database Views

	Entries in this log never expire.
<a href="#">vAgentConfiguration</a> (page 480)	Lists agent specific configuration data
<a href="#">vAgentLabel</a> (page 482)	
<a href="#">vAlertLog</a> (page 482)	Logs each alert sent out via email. Multiple rows per machine.
<a href="#">vBackupLog</a> (page 483)	Logs all backup related events
<a href="#">vConfigLog</a> (page 488)	Log of all configuration changes. One entry per change.
<a href="#">vNetStatsLog</a> (page 497)	Network statistics log from the Agent.
<a href="#">vNtEventLog</a> (page 497)	NT Event log data collected from each managed machine.
<a href="#">vPatchApprovalStatus</a> (page 497)	Show the approval status of a patch. There is one row for each active patch.
<a href="#">vPatchPolicy</a> (page 501)	Show the approval status of a patch. There is one row for each active patch in each patch policy.
<a href="#">vPatchPolicyMember</a> (page 502)	Lists all patch policies to which each machine ID is a member, if any.
<a href="#">vPatchStatus</a> (page 502)	Information on the state of all patches on a per machine basis. There is one row per patch for each machine.
<a href="#">vScriptLog</a> (page 505)	Log of procedure executions as viewed by the KServer.
<a href="#">vScriptStatus</a> (page 505)	Procedure status for each client.
<b>Ticketing Group</b>	
<a href="#">vTicketSummary</a> (page 508)	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.
<a href="#">vTicketNote</a> (page 508)	The notes associated with a ticket. Potentially multiple rows per ticket.
<a href="#">vTicketField</a> (page 507)	The fields associated with a ticket. The standard fields, category, status and priority are always attached to a ticket. User fields added will also be included in this view.
<b>Monitor Alarm Group</b>	
<a href="#">vMonitorAlarmAlert</a> (page 492)	The current list of alarms for all alerts.
<a href="#">vMonitorAlarmCounter</a> (page 493)	The current list of alarms for all monitor counters.
<a href="#">vMonitorAlarmProcess</a> (page 494)	The current list of alarms for all monitor processes.
<a href="#">vMonitorAlarmService</a> (page 494)	The current list of alarms for all monitor services.
<a href="#">vMonitorAlarmSNMP</a> (page 495)	The current list of alarms for all monitor SNMP Get objects.
<a href="#">vMonitorAlarmSystemCheck</a> (page 496)	The current list of alarms for all system checks.

## fnMissingPatchCounts\_UsePolicy / fnMissingPatchCounts\_NoPolicy

Both of these functions use the same parameters and return the same columns but each has different filtering based on patch approval policies.

fnMissingPatchCounts_UsePolicy	Returns the number of patches, using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the executive summary reports and the View Dashboard page under the Home tab. Only one row is returned.
--------------------------------	--

<b>fnMissingPatchCounts_NoPolicy</b>	Returns the number of patches, without using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the View Dashboard page under the Home tab. Only one row is returned.	
Parameter	Type	Purpose
@groupName	varchar	Machine group name; Use null or an empty string for all groups
@skipSubGroups	tinyint	When a group name is provided in the above parameter, determines whether to filter the results for only the one specified group or for the specified group and all of its subgroups: 0 = Use specified group and all of its subgroups 1 = Skip subgroups – use only the one specified group
Column	Type	Purpose
GroupName	varchar	Machine group name; Returns "All Groups" when the @groupName parameter is null or an empty string
WithSubgroups	varchar	YES when @skipSubGroups = 0 and for "All Groups" NO when @skipSubGroups = 1
FullyPatched	int	Count of fully patched machines in the group specified by the parameters
Missing12	int	Count of machines missing 1-2 patches in the group specified by the parameters
Missing35	int	Count of machines missing 3-5 patches in the group specified by the parameters
MissingMore5	int	Count of machines missing 5 or more patches in the group specified by the parameters
Unscanned	int	Count of unscanned machines in the group specified by the parameters
Unsupported	int	Count of machines for which patching is not supported in the group specified by the parameters

---

## fnOSCounts

<b>fnOSCounts</b>	Returns the types of operating systems and the counts for each for the specified machine group. Tabular data as seen in the OS pie charts in the executive summary reports and the View Dashboard page under the Home tab. Returns one row for each OSType.	
Parameter	Type	Purpose
@groupName	varchar	Machine group name; Use null or an empty string for all groups
@skipSubGroups	tinyint	When a group name is provided in the above parameter, determines whether to filter the results for only the one specified group or for the specified group and all of its subgroups: 0 = Use specified group and all of its subgroups 1 = Skip subgroups – use only the one specified group
Column	Type	Purpose
OSType	varchar	Operating system type such as "Win XP", "Win Vista", and "Mac OS X"
OSCount	int	Count of operating system type in the group specified by the parameters

---

## vAddRemoveList

vAddRemoveList		
Column Name	Type	Purpose
add/remove application list returned by the latest audit		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
applicationName	varchar(260), null	App name from the add/remove programs list

---

## vAdminNotesLog

vAdminNotesLog		
Column Name	Type	Purpose
Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
AdminLogin	varchar(100), not null	Admin logon name. (note: no not name this col adminName)
EventTime	datetime(3), not null	Time stamp string representing the time the action took place. Default is CURRENT_TIMESTAMP so nothing needs to be entered here.
NoteDesc	varchar(2000), not null	description of the action

---

## vAgentConfiguration

vAgentConfiguration		
Column Name	Type	Purpose
Logs each alert sent out via email. Multiple rows per machine		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent

groupName	varchar(100), null	Group Name used for each agent
firstCheckin	datetime(3), null	timestamp recording the first time this agent checked into the system
lastCheckin	datetime(3), null	timestamp recording the most recent time this agent checked into the system
currentUser	varchar(100), null	login name of the currently logged in user. Blank if no one logged in at this time
lastLoginName	varchar(100), not null	login name of the last user to log into this system
workgroupDomainType	tinyint(3), not null	0 (or Null) = unknown 1 = not joined to either 2 = member of workgroup 3 = member of domain 4 = domain controller
workgroupDomainName	nvarchar(32), null	The name of the workgroup or domain
lastReboot	datetime(3), null	timestamp when this system was last rebooted
agentVersion	int(10), null	version number of agent installed on this system
contactName	varchar(100), null	User contact name assigned to this agent
contactEmail	varchar(100), null	User email address assigned to this agent
contactPhone	varchar(100), null	Contact phone number assigned to this agent
contactNotes	varchar(1000), null	Notes associated with the contact information for this agent
enableTickets	int(10), not null	0 if this user does not have access to ticketing through the user interface
enableRemoteControl	int(10), not null	0 if this user does not have access to remote control through the user interface
enableChat	int(10), not null	0 if this user does not have access to chat through the user interface
loginName	varchar(100), not null	Login Name assigned to this user (if any) to access the system user portal interface.
credentialName	varchar(100), not null	The username of the credential set for this agent (if any)
primaryKServer	varchar(111), null	address:port agent connects to for its primary kserver connection
secondaryKServer	varchar(111), null	address:port agent connects to for its secondary kserver connection
quickCheckinSecs	int(10), null	interval in seconds between quick checkins
agentTempDir	varchar(200), null	The working directory used by the agent on this system

## vAgentLabel

vAgentLabel		Identifies the status of agents. Used for display purposes.
Column Name	Type	Purpose
displayName	varchar(201), null	The name of the machine ID.group name.
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
agentGuidStr	varchar(26), null	A string version of agentGuid. Some languages convert the large number numeric to exponential notation. This string conversion prevents that.
online	int(10), null	0 -> offline 1 -> online 2 -> online and user has not used the mouse or keyboard for 10 minutes or more. 198 -> account suspended 199 -> agent never checked in (template account)
transitionTime	datetime(3), null	Applies when online is either 0 or 2. <ul style="list-style-type: none"> <li>When online is 0, the time at which the Agent last checked in.</li> <li>When online is 2, the time when the machine was deemed idle (10 minutes after the last mouse or keyboard entry).</li> </ul>
timezoneOffset	int(10), null	The timezone offset for the agent as compared to universal time.
currentLogin	varchar(100), null	The login name of the current user.
toolTipNotes	varchar(1000), not null	The tooltip text displayed for a machine ID.
showToolTip	tinyint(3), not null	0 -> Do not show machine ID tool tips. 1 -> Do show tool machine ID tool tips.
agntTyp	int(10), not null	0 -> windows agent 4 -> mac agent 5 -> linux agent

## vAlertLog

vAlertLog		Logs each alert sent out via email. Multiple rows per machine
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent

groupName	varchar(100), null	Group Name used for each agent
EventTime	datetime(3), null	time stamp when the event was recorded
AlertEmail	varchar(1000), null	email address to send the alert to
AlertType	int(10), null	Alerts are one of several <a href="#">monitor types</a> (page 594). 1 - Admin account disabled 2 - Get File change alert 3 - New Agent checked in for the first time 4 - Application has been installed or deleted 5 - Agent Procedure failure detected 6 - NT Event Log error detected 7 - KServer stopped 8 - Protection violation detected. 9 - PCI configuration has been changed 10 - Disk drive configuration change 11 - RAM size changed. 12 - Test email sent by serverInfo.asp 13 - Scheduled report completed 14 - LAN Watch alert type 15 - agent offline 16 - low on disk space 17 - disabled remote control 18 - agent online 19 - new patch found 20 - patch path missing 21 - patch install failed 23 - Backup Alert
EmailSubject	varchar(500), null	Email subject line
EmailBody	varchar(4000), null	Email body

---

## vBackupLog

vBackupLog	Logs each alert sent out via email. Multiple rows per machine	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
EventTime	datetime(3), null	time stamp when the event was recorded
description	varchar(1000), null	description of the reported task
durationSec	int(10), null	number of seconds the reported task took to complete

## Database Views

statusType	int(10), null	<ul style="list-style-type: none"> <li>0: full volume backup</li> <li>1: offsite replication (obsolete)</li> <li>2: incremental volume backup</li> <li>3: offsite replication suspended (obsolete)</li> <li>4: offsite replication skipped because backup failed (obsolete)</li> <li>5: folder full backup</li> <li>6: offsite folder suspended (obsolete)</li> <li>7: differential volume backup</li> <li>8: folder incremental backup</li> <li>9: folder differential backup</li> <li>10: volume verification</li> <li>11: folder verification</li> <li>12: volume backup skipped because machine offline</li> <li>13: folder backup skipped because machine offline</li> <li>14: Informational</li> <li>15: Diff or Inc ran as full vol when last full vol not found</li> <li>16: Diff or Inc ran as full folder when last full folder not found</li> <li>17: volume backup cancelled</li> <li>18: folder backup cancelled</li> <li>19: volume image conversion (in KBU 3.0)</li> <li>20: volume synthetic full backup (in KBU 3.0)</li> <li>21: folder synthetic full backup (in KBU 3.0)</li> </ul>
result	int(10), null	<ul style="list-style-type: none"> <li>0: failure</li> <li>1: success</li> <li>2: archive incomplete</li> </ul>
imageSize	float(53), not null	The size of the backup.

## vBaseApplicationInfo / vCurrApplicationInfo

vBaseApplicationInfo vCurrApplicationInfo	audit results for installed applications. One entry per installed application found in the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
ProductName	varchar(128), null	Product name (e.g. Microsoft Office 2000)
ProductVersion	varchar(50), null	Version (e.g. 9.0.3822)
ApplicationName	varchar(128), null	Application name (e.g. Winword.exe)

manufacturer	varchar(128), null	Manufacturers name (e.g. Microsoft Corporation)
ApplicationDesc	varchar(512), null	Description (e.g. Microsoft Word for Windows)
LastModifiedDate	varchar(50), null	File date (e.g. 02/24/2000 17:23:44)
ApplicationSize	int(10), null	File size in bytes (e.g. 8810548)
DirectoryPath	varchar(256), null	Directory path on client desktop (e.g. C:\PROGRA~1\MICROS~4\OFFICE)

---

## vBaseCpuInfo / vCurrCpuInfo

vBaseCpuInfo vCurrCpuInfo	audit results for the CPU in a client desktop machine. One entry per audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
CpuDesc	varchar(80), null	CPU description (e.g. Pentium III Model 8)
CpuSpeed	int(10), null	CPU speed in MHz (e.g. 601)
CpuCount	int(10), null	Number of processors (e.g. 1)
TotalRam	int(10), null	Amount of RAM in MBytes (e.g. 250)

---

## vBaseDiskInfo / vCurrDiskInfo

vBaseDiskInfo vCurrDiskInfo	audit results for the logical disks found in a client desktop machine. One entry per logical disk from an audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
DriveLetter	varchar(8), null	Logical disk drive letter (e.g. C)

## Database Views

TotalSpace	int(10), null	Total MBytes on the disk (e.g. 28609 for 28.609 GB) May be null if unavailable.
UsedSpace	int(10), null	Number of MBytes used (e.g. 21406 for 21.406 GB). May be null if unavailable.
FreeSpace	int(10), null	Number of MBytes free (e.g. 21406 for 21.406 GB). May be null if unavailable.
DriveType	varchar(40), null	Fixed = hard disk Removable = floppy or other removable media CDROM Network = mapped network drive
VolumeName	varchar(32), null	Name assigned to the volume
FormatType	varchar(16), null	NTFS, FAT32, CDFS, etc.

---

## vBaseDriveManufacturer / vCurrDriveManufacturer

vBaseDriveManufacturer vCurrDriveManufacturer	Hardware audit results for the IDE & SCSI drives manufacturer and product info found in a client desktop machine. One entry per drive from an audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
DriveManufacturer	varchar(100), null	Manufacturer name (data currently has 8 characters max)
DriveProductName	varchar(100), null	Product identification (data currently has 16 characters max)
DriveProductRevision	varchar(40), null	Product revision (data currently has 4 characters max)
DriveType	varchar(9), not null	Type of disk drive found

---

## vBasePciInfo / vCurrPciInfo

vBasePciInfo vCurrPciInfo	Hardware audit results for the PCI cards manufacturer and product info found in a client desktop machine. One entry per PCI card from an audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent

groupName	varchar(100), null	Group Name used for each agent
VendorName	varchar(200), null	PCI Vendor Name
ProductName	varchar(200), null	PCI Product Name
ProductRevision	int(10), null	Product revision
PciBaseClass	int(10), null	PCI base class number
PciSubClass	int(10), null	PCI subclass number
PciBusNumber	int(10), null	PCI bus number
PciSlotNumber	int(10), null	PCI slot number

---

## vBasePrinterInfo / vCurrPrinterInfo

vBasePrinterInfo vCurrPrinterInfo	Printer audit results for the printers found for the current user logged on to a client desktop machine. One entry per printer from an audit of a client desktop. If no user is logged in, then Agent audits the printers for the system account, typically user.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
PrinterName	varchar(100), null	Name given to the printer. Same as shown in the Control Panels printer configuration window.
PortName	varchar(100), null	Name of the port to which the printer is attached. Same as shown in the Control Panels printer configuration window.
PrinterModel	varchar(100), null	Model name is the driver name retrieved from the printer information.

---

## vCollectionMember

vCollectionMember	Lists all collections each machine ID is a member of (if any).	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent

## Database Views

groupName	varchar(100), null	Group Name used for each agent
collectionName	varchar(100), not null	Collection Name

---

## vConfigLog

vConfigLog		Log of all configuration changes. One entry per change.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
EventTime	datetime(3), null	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year- month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
ConfigDesc	varchar(1000), null	Description of the change

---

## vkadComputers

vkadComputers		Contains active directory harvested computers
Column Name	Type	Purpose
Name	nvarchar(255), not null	AD Computer name
CanonicalName	nvarchar(255), not null	Canonical name
DomainName	nvarchar(255), null	Domain name
DistinguishedName	nvarchar(2048), null	AD distinguished name
OperatingSystem	nvarchar(30), null	Operating System
OperatingSystemVersion	nvarchar(20), null	Operating System version
LastLogon	datetime(3), null	Last time machine was rebooted
LastLogoff	datetime(3), null	Last time machine was shutdown
DNSHostName	nvarchar(255), null	Dns host name
WhenCreated	datetime(3), null	When the machine was made member of AD
WhenChanged	datetime(3), null	When the machine AD properties/role was updated

---

## vkadUsers

vkadUsers	Contains active directory harvested users.	
Column Name	Type	Purpose
logonName	nvarchar(255), not null	AD User name
CanonicalName	nvarchar(255), not null	Canonical name
DomainName	nvarchar(255), null	Domain name
DistinguishedName	nvarchar(2048), null	AD distinguished name
mail	varchar(200), null	User email address
phone	varchar(100), null	User phone number
givenName	nvarchar(50), null	User first name
sirName	nvarchar(50), null	User last name
LastLogon	datetime(3), null	Last time user logged on
LastLogoff	datetime(3), null	Last time user logged off
SAMAccountName	nvarchar(255), null	sAMAccount name (pre Win-2K account logon name)
Description	nvarchar(300), null	User account description
WhenCreated	datetime(3), null	When the user was made member of AD
WhenChanged	datetime(3), null	When the user AD properties was updated
PwdLastSet	datetime(3), null	When the user password was last set.

---

## vLicenseInfo

vLicenseInfo	License information collected during audit.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
Publisher	varchar(100), null	software publisher (usually in the Publisher reg value)
ProductName	varchar(100), null	Software title (usually in DisplayName value but may be the reg key title)
LicenseCode	varchar(100), null	License code (usually in the ProductID value)
ProductKey	varchar(100), null	Product key
LicenseVersion	varchar(100), null	version string returned by the scanner (if any)

## Database Views

InstallDate	varchar(100), null	install date string returned by the scanner (if any)
-------------	--------------------	--

## vMachine

vMachine		The information known about each client desktop machine.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	full machine name. Everything to the left of the left most decimal point is the machine name.
groupName	varchar(100), null	full group name for this account. Everything to the right of the left most decimal point is the group name.
Manufacturer	varchar(100), null	Manufacturer string (type 1)
ProductName	varchar(100), null	Product Name string (type 1)
MachineVersion	varchar(100), null	Version string (type 1)
SysSerialNumber	varchar(100), null	Serial Number string (type 1)
ChassisSerialNumber	varchar(100), null	Chassis Serial Number (type 3)
ChassisAssetTag	varchar(100), null	Chassis Asset Tag number (type 3)
BusSpeed	varchar(100), null	External Bus Speed (in MHz) (type 4)
MaxMemorySize	varchar(100), null	Maximum Memory Module Size (in MB) (type 16 - Maximum Capacity or if type 16 not available, Maximum Memory Module Size type 5)
MaxMemorySlots	varchar(100), null	Number of Associated Memory Slots (Number of Memory Devices in type 16 or if type 16 not available Number of Associated Memory Slots in type 5)
ChassisManufacturer	varchar(100), null	Chassis Manufacturer (type 3)
ChassisType	varchar(100), null	Chassis Type (type 3)
ChassisVersion	varchar(100), null	Chassis Ver (type 3)
MotherboardManufacturer	varchar(100), null	Motherboard Manufacturer (type 2)
MotherboardProductCode	varchar(100), null	Motherboard Product Code (type 2)
MotherboardVersion	varchar(100), null	Motherboard Version (type 2)
MotherboardSerialNumber	varchar(100)	Motherboard Serial Number (type 2)

	, null	
ComputerName	varchar(80), null	Name of the Computer
IpAddress	varchar(20), null	IP Address of the computer in a.b.c.d notation
SubnetMask	varchar(20), null	Subnet mask in a.b.c.d notation. String is empty if data is unavailable
DefaultGateway	varchar(20), null	Default gateway IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer1	varchar(20), null	DNS server #1s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer2	varchar(20), null	DNS server #2s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer3	varchar(20), null	DNS server #3s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer4	varchar(20), null	DNS server #4s IP address in a.b.c.d notation. String is empty if data is unavailable.
DhcpEnabled	int(10), null	0 -> Data is unavailable 1 -> DHCP on client computer is enabled 2 -> Disabled
DhcpServer	varchar(20), null	DHCP servers IP address in a.b.c.d notation. String is empty if data is unavailable.
WinsEnabled	int(10), null	0 -> Data is unavailable 1 -> WINS resolution on client computer is enabled 2 -> Disabled
PrimaryWinsServer	varchar(20), null	Primary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
SecondaryWinsServer	varchar(20), null	Secondary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
ConnectionGatewayIp	varchar(20), null	IP Address in a.b.c.d notation obtained by the Kserver as the source address of the Agent. This IP is the Agents network gateway and will be different from the IpAddress if the computer is behind NAT for example. String is empty if unavailable.
ipv6Address	varchar(40), null	The ipv6 address. Null, if no address is provided.
OsType	varchar(8), null	String contains OS type, such as NT4, 2000, NT3.51, or WIN32s. Derived from portions of MajorVersion, MinorVersion, and PlatformId.
OsInfo	varchar(150), null	String contains additional OS info, such as Build 1381 Service Pack 3. Derived from portions of BuildNumber and CsdVersion.
MajorVersion	int(10), null	Major version number from GetVersionEx() Windows function call.
MinorVersion	int(10), null	Minor version number from GetVersionEx() Windows function call. If PlatformId is Win32 for Windows, then a 0 MinorVersion indicates Windows 95. If PlatformId is Win32 for Windows, then then a MinorVersion > 0 indicates Windows 98.
MacAddr	varchar(40), null	String containing the physical address, i.e. the Media Access Control address, of the connection. A MAC address has the form of: 00-03- 47-12-65-77
LoginName	varchar(100), null	User name of the currently logged on user. This value is updated with every quick check in. The agent error log file is updated with

## Database Views

		each change.
timezoneOffset	int(10), not null	The timezone offset for the agent as compared to universal time.
agentInstGuid	varchar(4) not null	The unique portion of the path to the K2 (v6.0.0.0 and above) agent directory and to the service name as KA+vMachine.agentInstGuid.

## vMonitorAlarmAlert

vMonitorAlarmAlert		
Column Name	Type	Purpose
Listing of all alarms created by monitor alerts.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Group Name used for each agent
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	4 -> Monitor alert
EventLogType	int(10), null	Only applies to AlertType=6 (NT Event Log) 0 -> Application Event Log 1 -> System Event Log 2 -> Security Event Log
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
AlertType	int(10), not null	Alerts are one of several <a href="#">monitor types</a> (page 594). 1 - Admin account disabled 2 - Get File change alert 3 - New Agent checked in for the first time 4 - Application has been installed or deleted 5 - Agent Procedure failure detected 6 - NT Event Log error detected 7 - KServer stopped 8 - Protection violation detected. 9 - PCI configuration has been changed 10 - Disk drive configuration change 11 - RAM size changed. 12 - Test email sent by serverInfo.asp 13 - Scheduled report completed 14 - LAN Watch alert type 15 - agent offline 16 - low on disk space 17 - disabled remote control 18 - agent online 19 - new patch found 20 - patch path missing 21 - patch install failed 23 - Backup Alert

Message	varchar(3000), null	Message created from alarm, email message body
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
AdminName	varchar(100), null	User who assigned monitor alert to machine

---

## vMonitorAlarmCounter

vMonitorAlarmCounter		
Column Name	Type	Purpose
Listing of all alarms created by monitor counters.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Group Name used for each agent
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	0 -> Monitor Counter
MonitorName	varchar(100), not null	Name of monitor counter object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(3000), null	Message created from alarm, email message body
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm
AdminName	varchar(100), null	User who assigned monitor counter to machine

## vMonitorAlarmProcess

vMonitorAlarmProcess		Listing of all alarms created by monitor processes.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Group Name used for each agent
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	2 -> Monitor Process
MonitorName	varchar(100), not null	Name of monitor process object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(3000), null	Message created from alarm, email message body
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm, below are process values:
AdminName	varchar(100), null	0 -> Stopped 1 -> Running

## vMonitorAlarmService

vMonitorAlarmService		Listing of all of the alarms created by monitor services.
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar	Machine Name used for each agent

GroupName	varchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	0 -> Monitor Service
MonitorName	varchar	Name of monitor service object
AlarmType	smallint	0 -> Alarm 1 -> Trending
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm, below are service values: -1 -> Does not exist 0 -> Reserved 1 -> Stopped 2 -> Start Pending 3 -> Stop Pending 4 -> Running 5 -> Continue Pending 6 -> Pause Pending 7 -> Paused
AdminName	varchar	User who assigned monitor service to machine

---

## vMonitorAlarmSNMP

vMonitorAlarmSNMP		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Group Name used for each agent
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	3 -> Monitor SNMP Get
MonitorName	varchar(100), not null	Name of monitor SNMP Get object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(3000), null	Message created from alarm, email message body

## Database Views

AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm, if the return value of the SNMP Object Get command is a string the value will be the the Message
SNMPName	varchar(50), null	Name returned from SNMP Device on scan
SNMPCustomName	varchar(100), null	Custom name for SNMP Device
AdminName	varchar(100), null	User who assigned monitor SNMP Get to machine

## vMonitorAlarmSystemCheck

vMonitorAlarmSystemCheck		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Group Name used for each agent
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	5 -> Monitor system check
SystemCheckType	int(10), null	1 -> Web Server 2 -> DNS Server 4 -> Port Connection 5 -> Ping 6 -> Custom
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Parameter1	varchar(1000), null	First parameter used in system check
Parameter2	varchar(1000), null	(Optional) Second parameter used by system check
Message	varchar(3000), null	Message created from alarm, email message body
AlertSubject	varchar(500)	Subject of alarm and email subject

	, null	
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
AdminName	varchar(100), null	User who assigned of monitor counter to machine

---

## vNetStatsLog

vNetStatsLog		network statistics log from the Agent
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
EventTime	datetime(3), null	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year-month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
BytesRcvd	int(10), null	Number of bytes received during this statistics period
BytesSent	int(10), null	Number of bytes sent during this statistics period
ApplicationName	varchar(800), null	Application name using the network

---

## vNtEventLog

vNtEventLog		Event log data collected from each managed machine
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent

## Database Views

logType	int(10), null	1 -> Application Log 2 -> Security Log 3 -> System Log
eventType	int(10), null	1 -> Error 2 -> Warning 4 -> Informational 8 -> Success Audit 16 -> Failure Audit
eventTime	datetime(3), null	Time the event occurred
ApplicationName	nvarchar(200), null	event log source
EventCategory	nvarchar(200), null	event log category
eventId	int(10), null	event log event ID
username	nvarchar(200), null	event log user
computerName	nvarchar(200), null	event log computer name
EventMessage	nvarchar(2000), null	event log message

---

## vOnBoardDeviceInfo

vOnBoardDeviceInfo	Data collected by KaSmBios.exe during an audit for on-board device information. There is one row per active slot. All information is retrieved from Type 10.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
DeviceType	varchar(100), null	Device Type
DeviceDesc	varchar(100), null	Device Description

---

## vPatchApprovalStatus

vPatchApprovalStatus	Show the approval status of a patch. There is one row for each active patch.	
Column Name	Type	Purpose

patchDataId	int(10), not null	Unique identifier for this patch within the database
KBArticle	varchar(12), not null	Microsoft knowledge base article number
SecurityBulletin	varchar(40), not null	Microsoft security bulleting number
Title	varchar(250), not null	Patch title
UpdateClassificationId	smallint(5), not null	Numeric representation of the patch update classification; included to make filtering easier; Values are: 100 = Critical Security Update (High Priority) 101 = Important Security Update (High Priority) 102 = Moderate Security Update (High Priority) 103 = Low Security Update (High Priority) 104 = Non-rated Security Update (High Priority) 110 = Critical Update (High Priority) 120 = Update Rollup (High Priority) 200 = Service Pack (Optional) 210 = Update (Optional) 220 = Feature Pack (Optional) 230 = Tool (Optional)
UpdateClassification	varchar(43), not null	Textual representation of the patch update classification
Product	varchar(300), null	Product this to which this patch is associated
PublishedDate	datetime(3), null	Date that this patch was last update by Microsoft, if available
Language	varchar(30), not null	Language support for the patch
numApproved	int(10), null	Number of patch policies in which this patch is approved
numDenied	int(10), null	Number of patch policies in which this patch is denied
numPending	int(10), null	Number of patch policies in which this patch is pending approval
InstallationWarning	varchar(20), not null	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.

---

## vPatchConfiguration

<b>vPatchConfiguration</b>	Provides the various patch-related configurations. There is one row per machine.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Group Name used for each agent

## Database Views

PatchScanTypeSetting	int(10), not null	Type of patch scan: -1 = OS not supported for patch scans 0 = Legacy Patch Scan 1 = WUA Patch Scan (32-bit) 2 = WUA Patch Scan (64-bit)
PatchScanType	varchar(300), null	Type of patch scan description
RebootSetting	int(10), not null	Post patch installation reboot action: 0 = Reboot immediately 1 = Ask - Do nothing if user does not respond in <RebootWarnMinutes> minutes 2 = Do not reboot after update; If exists, send email to <RebootWarningEmailAddress> 3 = Ask - Reboot if user does not respond in <RebootWarnMinutes> minutes 4 = Warn user that machine will reboot in <RebootWarnMinutes> minutes 5 = Skip reboot if user logged in 6 = Reboot on <RebootDay> at <RebootTime> after install 7 = Ask to reboot every <RebootWarnMinutes> minutes
RebootAction	varchar(143), null	Post patch installation reboot action description
PreRebootScript	varchar(260), not null	scriptId of script to execute immediately before the reboot step in the Patch Reboot script
PostRebootScript	varchar(260), not null	scriptId of script to execute immediately after the patch reboot (from scriptAssignmentReboot)
RebootWarnMinutes	int(10), null	Warning wait period in minutes for RebootSetting 1,3,4,7
RebootDay	int(10), null	Day to force patch reboot for RebootSetting 6: 0 = Everyday 1 = Sunday 2 = Monday 3 = Tuesday 4 = Wednesday 5 = Thursday 6 = Friday 7 = Saturday
RebootTime	varchar(10), null	Time to force patch reboot for RebootSetting 6
RebootWarningEmailAddress	varchar(100), null	Email address to send email for post patch installation reboot for RebootSetting 2
FileSourceSetting	int(10), not null	Patch installation file source: 0 = From Internet 1 = From system server 2 = From file server
FileSourceConfig	varchar(166), not null	Patch installation file source description
UseAgentTempDirOnDriveMostFreeSpace	int(10), not null	Destination for downloaded patch file: 0 = Use configured Agent working drive/directory 1 = Use configured Agent working directory on local disk drive having most free space

DeleteAfterInstall	int(10), not null	Delete downloaded patch file after installation: 0 = Do not delete 1 = Delete
FileSourceMachineld	varchar(201), null	MachineGroup_ID for the file server for FileSourceSetting 2
FileSourceUNCPath	varchar(300), null	UNC path for the file server for FileSourceSetting 2
FileSourceLocalPath	varchar(300), null	Local machine path for the file server for FileSourceSetting 2
UseInternetSourceAsFallback	int(10), null	If file server not accessible, fall back to use the Internet for FileSourceSetting 2
WinAutoUpdateSetting	int(10), not null	Windows Automatic Update setting 0 = Windows automatic Updates configuration set; Cannot be changed by user on the machine 1 = Windows automatic Updates disabled; Cannot be changed by user on the machine 2 = User control
WinAutoUpdateConfig	varchar(93), null	Windows Automatic Update description

---

## vPatchPolicy

<b>vPatchPolicy</b>	Show the approval status of a patch. There is one row for each active patch in each patch policy.	
<b>Column Name</b>	<b>Type</b>	<b>Purpose</b>
patchDataId	int(10), not null	Unique identifier for this patch within the database
Policy	varchar(100), null	Name of patch policy
KBArticle	varchar(12), not null	Microsoft knowledge base article number
SecurityBulletin	varchar(40), not null	Microsoft security bulleting number
Title	varchar(250), not null	Patch title
UpdateClassificationId	smallint(5), not null	Numeric representation of the patch update classification; included to make filtering easier; Values are: 100 = Critical Security Update (High Priority) 101 = Important Security Update (High Priority) 102 = Moderate Security Update (High Priority) 103 = Low Security Update (High Priority) 104 = Non-rated Security Update (High Priority) 110 = Critical Update (High Priority) 120 = Update Rollup (High Priority) 200 = Service Pack (Optional) 210 = Update (Optional) 220 = Feature Pack (Optional) 230 = Tool (Optional)

## Database Views

UpdateClassification	varchar(43), not null	Textual representation of the patch update classification
Product	varchar(300) , null	Product this to which this patch is associated
PublishedDate	datetime(3), null	Date that this patch was last update by Microsoft, if available
Language	varchar(30), not null	Language support for the patch
ApprovalStatusId	smallint(5), not null	Numeric representation of the patch approval status; included to make filtering easier; Values are: 0 = Approved 1 = Denied 2 = Pending Approval
ApprovalStatus	varchar(16), not null	Textual representation of the patch approval status
Admin	varchar(100) , not null	Name of user that made the most recent status change ("*System*" indicates that the approval status was set by the system based upon patch policy default approval status or by KB Override)
Changed	datetime(3), not null	Timestamp of most recent approval status change
InstallationWarning	varchar(20), not null	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.
StatusNotes	varchar(500) , not null	Notes added by Admin concerning the patch approval status

---

## vPatchPolicyMember

vPatchPolicyMember	Lists all patch policies to which each machine ID is a member, if any.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201) , null	A concatenated representation of the machine id and the group id to which it is associated
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent
machName	varchar(100) , null	Machine Name used for each agent
groupName	varchar(100) , null	Group Name used for each agent
PolicyName	varchar(100) , not null	Patch Policy Name

---

## vPatchStatus

vPatchStatus	Shows the state of all patches on a per machine basis. There is one row per patch for each machine.	
Column Name	Type	Purpose

Machine_GroupID	varchar(201), not null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), not null	Machine name used for each agent.
GroupName	varchar(100), not null	Group Name used for each agent,
KBArticle	varchar(10), not null	Microsoft KB article number reported from the patch scanner.
SecurityBulletin	varchar(40), not null	Bulletin ID string reported from the patch scanner.
Title	varchar(250), not null	Update title.
Product	varchar(300), null	Product to which patch is associated
Language	varchar(30) null	Language of the product.
UpdateClassification	smallint(5), not null	Update classification: 100 -> Security Update – Critical 101 -> Security Update – Important 102 -> Security Update – Moderate 103 -> Security Update – Low 104 -> Security Update – Unrated 110 -> Critical Update 120 -> Update Rollup 200 -> Service Pack 210 -> Update 220 -> Feature Pack 230 -> Tool 900 -> Unclassified 999 -> Kaseya Patch Test
UpdateClassificationDescription	varchar(43), not null	Same as UpdateClassification in string format.
ReleaseDate	datetime, null	Patch release date
ApprovalStatus	smallint, not null	0 -> approved 1 -> disapproved 2 -> pending approval
ApprovalStatusDescription	varchar(16), not null	Same as ApprovalStatus in string format.
InstallSeparate	tinyint(3), not null	0 -> this can be installed together with other patches 1 -> this must be installed separately (its own reboot) from other patches
IsSuperseded	tinyint(3), not null	0 -> update is not superseded 1 -> update is superseded by a subsequent update
PatchAppliedFlag	int(10), not null	0 -> patch has not been applied 1 -> patch has been applied

## Database Views

PatchStatus	int(10), not null	0 -> this patch not scheduled to be installed 1 -> schedule this patch for install. Flags used to bundle all patches into a single script. Set when installation scripts are generated. 2 -> patch install failed, no alert sent 3 -> patch install failed and alert has been sent 4 -> patch installed and awaiting a reboot to reconfirm 5 -> schedule rollback for this patch 6 -> "/install-as-user" patch not installed; User not logged in 7 -> Office patch not installed; User request to install declined or timed out 8 -> patch get/install failed, client login credential is invalid
PatchStatusDescription	varchar(42), not null	Same as PatchStatus is string format.
PendingManualInstall	int(10), not null	Patch selected by manual update (Machine Update or Patch Update): 0 -> not selected for installation 1 -> selected for installation
PatchIgnoreFlag	int(10), not null	0 -> process this patch 1 -> ignore this patch
InstallationWarning	varchar(22), not null	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', "Internet-based Install", or an empty string.
InstallDate	datetime(3), null	timestamp when this patch was applied by the VSA
InstalledBy	varchar(100), null	Name of admin (if we installed the patch) or value from registry (if scanner returned the value)
Description	varchar(1500), null	Patch description
UninstallNotes	varchar(1500), null	Uninstall notes for the patch

---

## vPortInfo

<b>vPortInfo</b>	Data collected by KaSmBios.exe during an audit on port connector information. There is one row per active slot. All information is retrieved from Type 8.	
<b>Column Name</b>	<b>Type</b>	<b>Purpose</b>
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
InternalDesc	varchar(100), null	Internal Description
ExternalDesc	varchar(100), null	External Description

ConnectionType	varchar(100), null	Connection Type
PortType	varchar(100), null	Port Type

---

## vScriptLog

vScriptLog		Log of procedure executions as viewed by the KServer
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
EventTime	datetime(3), null	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year- month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
ScriptName	varchar(260), null	Name of procedure
ScriptDesc	varchar(1000), null	Event description
AdminName	varchar(100), null	Admin name that scheduled this procedure.

---

## vScriptStatus

vScriptStatus		procedure status for each client
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
scriptName	varchar(260), null	Name of procedure
LastExecTiime	datetime(3), null	Time stamp string representing the last time that the procedure was executed

## Database Views

lastExecStatus	varchar(100), null	Status of the last execution. The string will be one of the following: Procedure Summary: Success <ELSE or THEN> Procedure Summary: Failed <ELSE or THEN> in # step <ELSE or THEN> is replaced with the respective word ELSE or THEN. # is replaced by the number of steps that failed in the procedure (not useful unless allowing the processing to continue after a failure) step is replaced by the work steps if the procedure failed more than 1 step.
AdminLogin	varchar(100), null	Admin name that last scheduled this procedure. (Dont name this column adminName because that is a primary key used by database migration. adminName and emailAddr should not appear in the same table.

## vSystemInfo

vSystemInfo		Data collected by the <a href="#">System Info</a> (page 140) function.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
Manufacturer	varchar(100), null	System manufacturer string
Product Name	varchar(100), null	Name or model number of the machine supplied by the manufacturer
System Version	varchar(100), null	Machine version string
System Serial Number	varchar(100), null	Machine serial number string entered by the manufacturer
Chassis Serial Number	varchar(100), null	Serial number string supplied by the manufacturer
Chassis Asset Tag	varchar(100), null	Asset tag string supplied by the manufacturer
External Bus Speed	varchar(100), null	Motherboard bus speed
Max Memory Size	varchar(100), null	Max memory this system may be configured with
Max Memory Slots	varchar(100), null	Max number of memory slots this system has
Chassis Manufacturer	varchar(100), null	Name of manufacturer of the chassis
Chassis Type	varchar(100), null	system chassis type
Chassis Version	varchar(100), null	version string of the chassis
Motherboard Manufacturer	varchar(100), null	Name of motherboard manufacturer

Motherboard Product	varchar(100), null	Motherboard model name
Motherboard Version	varchar(100), null	Motherboard version number
Motherboard Serial Num	varchar(100), null	Motherboard serial number
Processor Family	varchar(100), null	processor family name
Processor Manufacturer	varchar(100), null	processor manufacturer name
Processor Version	varchar(100), null	processor version string
CPU Max Speed	varchar(100), null	max speed of this processor
CPU Current Speed	varchar(100), null	configured speed of this processor

\* Custom columns defined using Audit > **System Info** (page 140) display in the **vSystemInfoManual** (page 507) database view.

---

## vSystemInfoManual

vSystemInfo	Custom fields and values added to the <b>System Info</b> (page 140) function.	
Column Name	Type	Purpose
agentGuid	numeric(26, 0), not null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
fieldName	nvarchar(100), not null	The name of the custom field.
fieldValue	varchar(100), null	The value of the custom field.

---

## vTicketField

vTicketField	Each ticket will have a set of fields associated with it. Three of these fields are standard fields, status, priority, and category. Also, a series of user fields can be added that will also be seen in this view. Each field has a datatype. All lists are stored as integer values. The view vTicketField has the associated text for each list value.	
Column Name	Type	Purpose
TicketID	int(10), null	unique trouble ticket ID number
TicketLabel	varchar(50), null	The label of the field
IntegerValue	int(10), null	The value of a integer field
NumberValue	numeric(15, 4), null	The value of a number field
StringValue	varchar(500)	The value of a string field

## Database Views

	, null	
ListValue	varchar(50), null	The value of a list field

---

## vTicketNote

vTicketNote	Trouble ticket notes are stored in the database. Each ticket summary can have multiple notes. There is a timestamp that identifies the order they were attached.	
Column Name	Type	Purpose
TicketID	int(10), null	unique trouble ticket ID number
author	varchar(100), null	person who wrote this note in the ticket
TicketNoteTime	datetime(3), not null	Timestamp identifying when the note was added
TicketNote	varchar(2000), not null	Contents of the ticket note
HiddenNote	int(10), not null	0 if the note is visible. 1 if the note is hidden.

---

## vTicketSummary

vTicketSummary	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.	
Column Name	Type	Purpose
TicketID	int(10), not null	unique trouble ticket ID number
Machine_GroupID	varchar(100), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
TicketSummary	varchar(256), not null	summary string briefly describing the ticket
Assignee	varchar(100), null	Admin name this ticket is assigned to
CreatedBy	varchar(100), null	admin name (or machine ID if entered by user) of the person that created this ticket
CreationDate	datetime(3), null	timestamp when the ticket was created
DueDate	datetime(3), null	ticket due date

LastModifiedDate	datetime(3), null	Date of the most recent note entered for this ticket
ResolutionDate	datetime(3), null	timestamp when the ticket was closed
UserName	varchar(100), null	The name of the submitter
UserEmail	varchar(200), null	The email address of the submitter
UserPhone	varchar(100), null	The phone number of the submitter

---

## vUptimeHistory

vUptimeHistory	Data collected for the uptime history report. Use in conjunction with the getMachUptime web service	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
eventTime	datetime(3), null	timestamp of the beginning of the time segment
duration	int(10), null	Number of seconds this time segment lasted
type	int(10), null	1 – Agent on but cannot connect to kserver 2 – Agent on and connected to kserver 3 – Agent off normally 4 – Abnormal agent termination 5 – Agent alarms suspended (do not count suspended time when computing total uptime (function getMachUptime) 6 – Suspend ended
loginName	varchar(100), null	Name of the user logged on during this time segment. (SYSTEM if no one was logged on).

---

## vProAssetDetails

vProAssetDetails	Lists information about a vPro enabled machine, including manufacturing details about the motherboard.	
Column Name	Type	Purpose
agentGuid	numeric(26,0), null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
displayName	varchar(201), null	If the vPro machine has an agent on it then the display name is

## Database Views

		the machine.GroupId of a normal agent listing. Otherwise it is blank.
hostName	varchar(255), null	name of the machine on the LAN
computerName	varchar(255), null	holds the computer name found in the OS
assetId	varchar(50), not null	the asset Id is part of the basic hardware information
computerModel	varchar(65), null	Model designation of the computer
computerManufacturer	varchar(65), null	Manufacturer of the computer
computerVersion	varchar(65), null	Version number of the computer
computerSerialNumber	varchar(65), null	Serial number of the computer
mbManufacturer	varchar(65), null	Motherboard manufacturer
mbProductName	varchar(65), null	Product name of the motherboard
mbVersion	varchar(65), null	Version number of the motherboard
mbSerialNumber	varchar(65), null	Serial number of the motherboard
mbAssetTag	varchar(65), null	Asset tag for the motherboard
mbReplaceable	tinyint(3), null	True or false if the motherboard is replaceable
biosVendor	varchar(65), null	Vendor for the BIOS
biosVersion	varchar(65), null	Version number of the BIOS
biosReleaseDate	datetime(3), null	BIOS release date
biosSupportedFunctions	varchar(1000), null	List of BIOS supported features
ipAddress	varchar(19), null	ipAddress of the vPro machine used by power management and remote ISO boot

## Chapter 14

# API Web Services

### In This Chapter

VSA API Web Service	513
Agent Procedure API Web Service	552
Monitoring API Web Service	554
KSD API Web Service	559

**About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

---

# VSA API Web Service

## In This Section

VSA API Web Service - Overview	513
VSA API Web Service - Operations	522

## VSA API Web Service - Overview

The VSA [API Web Service](#) provides a generalized interface for a client to programmatically interface to the VSA. This API facilitates a client being able to interface a third party package. The API focuses on the following services:

- **Connect** - This service facilitates the consumer of the API to authenticate and receive a GUID to use throughout the communication. This GUID ages off similarly to how users age off.
- **Tickets** - This service provides basic facilities for the user to be notified of new tickets. This facility allows users to update fields on a ticket.
- **Alarms** - This service provides basic facilities for the user to be notified of new alarms and mark an alarms as closed.
- **Machines** - This service provides a request to collect a set of data about one or more machines.

The VSA [API Web Service](#) is based on the [Web Services Description Language \(WSDL\)](#). The WSDL displays in a browser and provides an abstract description of the data being exchanged to and from a web service. A client program connecting to a web service can read the WSDL to determine what functions are available on the server. Any special datatypes used are embedded in the WSDL file in the form of XML Schema. The client can then use SOAP to actually call one of the functions listed in the WSDL.

The following is an example of vsaWS output:

### KaseyaWS

---

#### GetMachine

Returns machine detail for the submitted Machine\_GroupID.

**Test**

The test form is only available for requests from the local machine.

**SOAP 1.1**

The following is a sample SOAP 1.1 request and response. The **placeholders** shown need to be replaced with actual values.

```

POST /vsaWS/kaseyaWS.asmx HTTP/1.1
Host: 192.168.214.224
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "KaseyaWS/GetMachine"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetMachine xmlns="KaseyaWS">
      <req>
        <Machine_GroupID>string</Machine_GroupID>
        <SessionID>decimal</SessionID>
      </req>
    </GetMachine>
  </soap:Body>
</soap:Envelope>

HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetMachineResponse xmlns="KaseyaWS">
      <GetMachineResult>
        <Machine_GroupID>string</Machine_GroupID>
        <machName>string</machName>
        <groupName>string</groupName>
        <Manufacturer>string</Manufacturer>
        <ProductName>string</ProductName>
        <MachineVersion>string</MachineVersion>
      </GetMachineResult>
    </GetMachineResponse>
  </soap:Body>
</soap:Envelope>

```

## Enabling VSA API Web Service

To enable the VSA API Web Service:

- Display the System > **Configure** (page 412) page in the VSA.
- Check the **Enable VSA API Web Service** checkbox.
- Access the VSA API web service using `http://<your-KServer>/vsaWS/KaseyaWS.asmx`

**Note:** The KSD API Web Service describes additional **Service Desk API** operations.

## Special Fields

The following fields are included in the response to every request.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

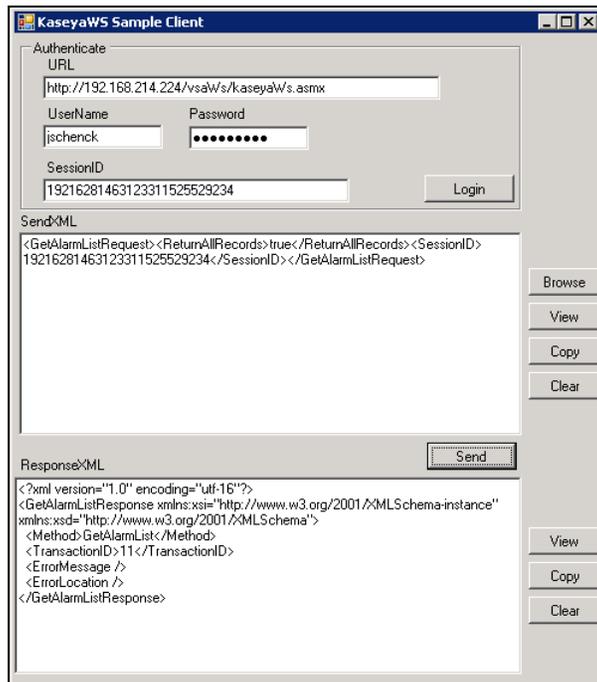
A **Session ID** is created by the web service and returned to the client the first time a method is invoked by the client. That same session ID must be returned by the client with every method invoked during the session. The SessionID is only valid when received from the same IP address the authentication

originates from.

## VSA API Web Service Sample Client - C# GUI application

A GUI test client and set of test XMLs are distributed with the VSA API Web Service to help you familiarize yourself with the various API operations. The C# source code for the VSA API Web Service **Sample Client** is provided to you without restriction. You can use it to see how the client was constructed and incorporate any part of its code into your own application.

**Note:** An ASP page text client (page 516) is also provided.



To run the sample client:

1. Run the sample client located on your KServer:  
`<Install Dir>\vsaWs\TestClient\KaseyaWStestClient.exe`
2. Enter the **UserName** and **Password** of a user authorized to connect with the KServer.

**Note:** This is the same username and password that an administrator uses to login into the KServer.

3. Click the **Login** button to display a value in the **SessionID** field.
4. Click the **Browse** button to select a test XML file. This populates the **SendXML** textbox with the text of the XML file.

**Note:** You do not have to enter a value between the **<SessionID>** element tags of the test XML message. The **Sample Client** automatically inserts the displayed **SessionID** into any XML message when you click the **Send** button.

5. Click the **Send** button to send the XML message to the target URL. A response XML message displays in the **ResponseXML** textbox.

## VSA API Web Service Sample Client - ASP Page

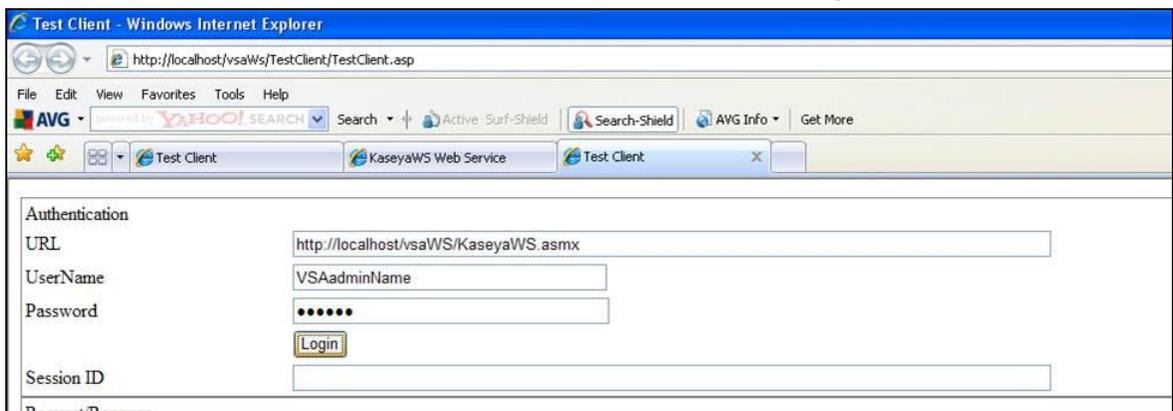
A test client ASP page is also distributed with the VSA API Web Service to help you familiarize yourself with the various API operations. You can use it to see how the ASP client was constructed and incorporate any part of its code into your own application. Users can browse to the actual /vsaWS/KaseyaWS.asmx page of any Kserver, select a web method and copy and paste the exact XML SOAP request structure specified in the WSDL.

Authentication is in its own frame at the top of the page. The sessionID from a successful authentication is exposed and can be copied and pasted in subsequent XML requests.

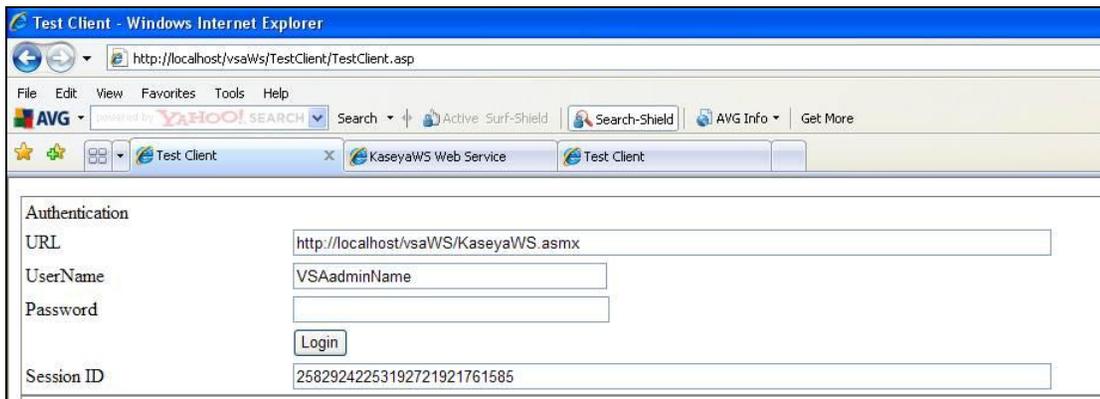
**Note:** This page does not automatically incorporate the displayed sessionID into subsequent request statements like the **C# GUI Test Client** (page 515) does.

### Example 1: Authentication

1. Access the VSA API web service asp test client using  
<http://<your-KServer>/vsaWS/TestClient/TestClient.asp>
2. Enter a valid VSA administrator UserName and Password and click Login.

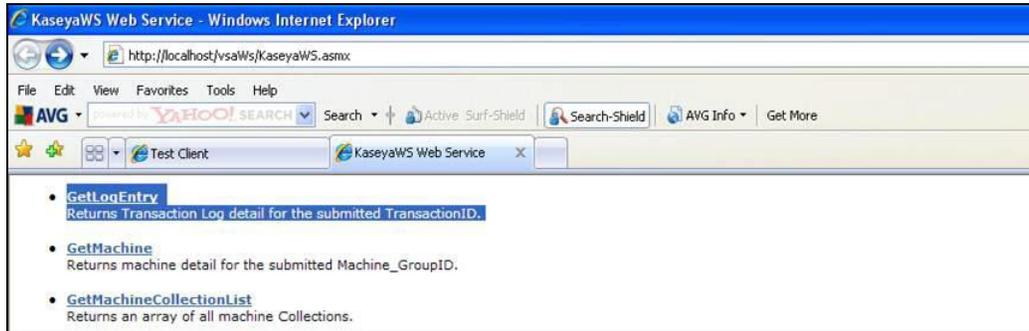


The Session ID textbox is populated with the session ID generated by your logon. You will need to copy and paste this session ID into subsequent XML requests.

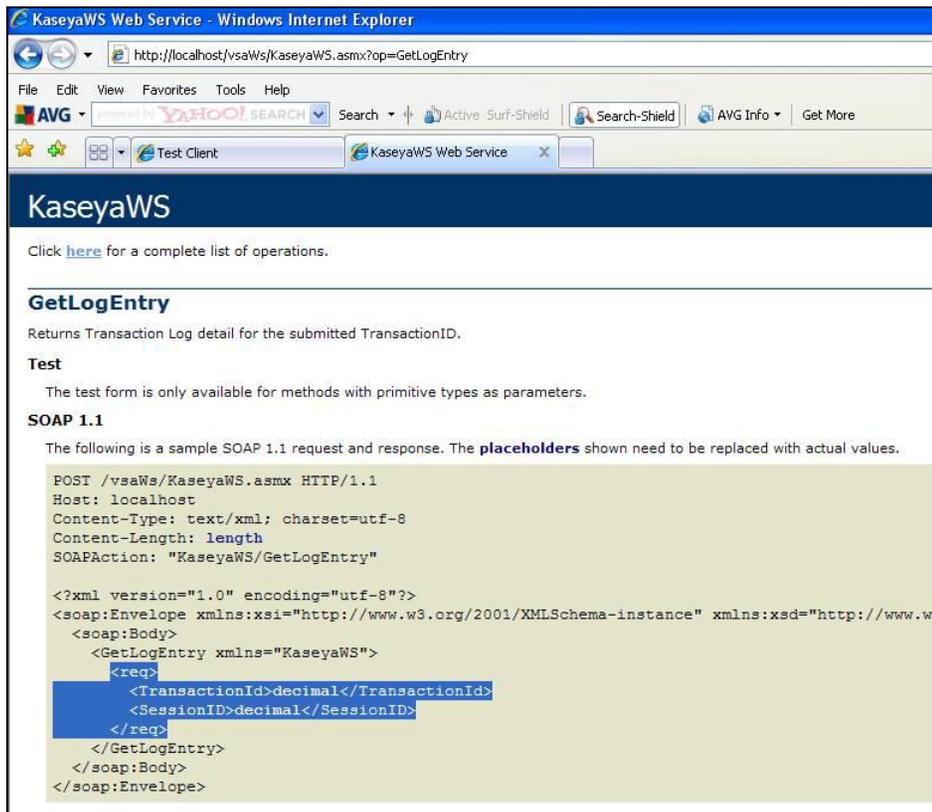


## Example 2 - Creating a Get Request

1. In a second browser window, use the /vsaWS/KaseyaWS.asmx page to select a method, such as GetLogEntry.

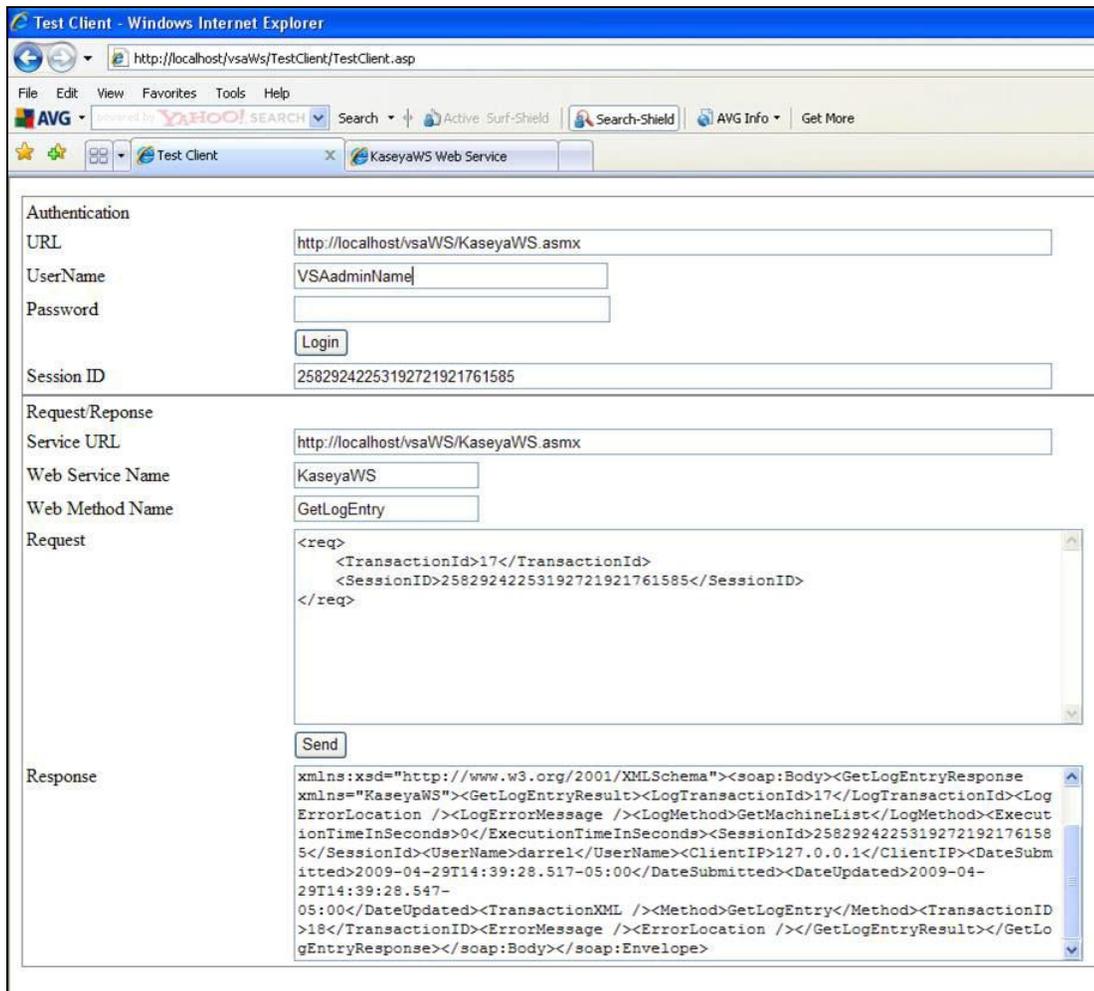


2. Each method displays the XML SOAP structure for that method's request. Copy just the portion of the method's request structure that starts with <req> and ends with </req>.



- Paste the request structure into the Request pane of the TestClient.asp page. Enter the name of the method in the Web Method Name field. Replace the placeholder decimal with the sessionID string you obtained during authentication. Replace any other placeholder content with valid data as required. Then click the Send button.

**Note:** The <BrowserIP></BrowserIP> element in any method can be ignored. The <BrowserIP> element helps to provide single-signon coordination with the VSA, and can be ignored in a testing environment where single-signon is not the focus.



The results display in the Response pane.

# VSA API Web Service Security

## General

The VSA API Web Service is accessible, by default, from any IP address in the world using any valid VSAUser credentials. In this default configuration, valid username /password combinations are considered for authentication originating from any machine.

In any configuration, the `hash.dll` provided by the VSA must be used to encrypt the password for submission. Implementation details for the `hash.dll` are contained in the sample source code provided.

Once a successful **Authentication** request issues a SessionID, this SessionID must be submitted with every service invocation, and is only valid when received from the IP address it was issued to. The issued SessionID expires after a period of inactivity.

Security can be enhanced by preparing and deploying an `AccessRules.xml` file. This file is used by the VSA API Web Service to define access rules based on the IP addresses requests are received from. IP filtering is a mechanism commonly used in business-to-business systems to ensure that requests are honored only from the partner's servers.

The `AccessRules.xml` file is divided into three sections:

- Default Access Rules
- IP Ranges
- User Mapping

**Note:** 127.0.0.1 (localhost) always has access for any account, regardless of configuration.

## XML Structure

```
<AccessRules>
  <DefaultAccessRules>
    <GrantAnyIPToUndefinedUsers/>
    <GrantAllIPRangesToUndefinedUsers/>
    <DenyAccessToUndefinedUsers/>
  </DefaultAccessRules>
  <IPRanges>
    <IPRange RangeID="" FromIPAddress="" ToIPAddress="" RangeDescription=""/>
    <IPRange RangeID="" FromIPAddress="" ToIPAddress="" RangeDescription=""/>
  </IPRanges>
  <UserMapping>
    <User UserName="" RangeID="" GrantAllRanges="" GrantAnyIP="" DenyAccess=""/>
    <User UserName="" RangeID="" GrantAllRanges="" GrantAnyIP="" DenyAccess=""/>
  </UserMapping>
</AccessRules>
```

## Default Access Rules

The elements in this section define the access rules for those accounts that are not specifically addressed in the User Mapping section.

`<GrantAnyIPToUndefinedUsers/>` true/false

true: Any user not in UserMapping gets access from any IP address.

`<GrantAllIPRangesToUndefinedUsers/>` true/false

true: Any user not in UserMapping gets access from any IP address contained in IPRanges.

`<DenyAccessToUndefinedUsers/>` true/false

true: Any user not in UserMapping denied access.

## IP Ranges

This section is used to define specific machines, or ranges of machines, by IP, that are used to assign user access.

`RangeID="integer"`

## API Web Services

An arbitrary, user assigned integer used to refer to the Range in UserMapping.

`FromIPAddress="string"`

Starting IP address, inclusive. First three positions of the quartet must match ToIPAddress.

`ToIPAddress=" string"`

Ending IP address, inclusive. First three positions of the quartet must match FromIPAddress.

`RangeDescription=" string"`

Description of the IP Range. For example: "Production Servers".

## User Mapping

`UserName="string"`

The VSA Admin name. The VSA API Web Service uses the same credentials and password encryption as VSA. So, if you change your password in VSA, be sure to change it in your VSA API Web Service client implementation, as well.

`RangeID="integer"`

Used to point to a defined IP Range in the IP Ranges section. A user can have multiple UserMapping elements to express all the IP Ranges he has access from. Not used when one of the Grant / Deny attributes below are used.

`GrantAllRanges="true/false"`

true: User has access from any range defined in the IP Ranges section.

`GrantAnyIP=" true/false"`

true: User has access from any IP address.

`DenyAccess=" true/false"`

true: User has no access at all.

## Sample Access Configuration XML

```
<AccessRules>
  <DefaultAccessRules>
    <GrantAnyIPToUndefinedUsers>>false</GrantAnyIPToUndefinedUsers>
    <GrantAllIPRangesToUndefinedUsers>>false</GrantAllIPRangesToUndefinedUsers>
    <DenyAccessToUndefinedUsers>>true</DenyAccessToUndefinedUsers>
  </DefaultAccessRules>
  <IPRanges>
    <IPRange RangeID="1" FromIPAddress="192.168.214.01" ToIPAddress="192.168.214.10"
RangeDescription="Partner X Production Web Farm"/>
    <IPRange RangeID="2" FromIPAddress="192.168.15.102" ToIPAddress="192.168.15.102"
RangeDescription="Senior Developer Machine"/>
    <IPRange RangeID="3" FromIPAddress="192.168.15.105" ToIPAddress="192.168.15.109"
RangeDescription="Sales Demo Machines"/>
    <IPRange RangeID="4" FromIPAddress="192.168.210.35" ToIPAddress="192.168.210.35"
RangeDescription="Internal QA Machine"/>
  </IPRanges>
  <UserMapping>
    <User UserName="B2BMasterAdmin" RangeID="1" GrantAllRanges="false"
GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="DevTestAccount" RangeID="2" GrantAllRanges="false"
GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="SalesTestAccount" RangeID="3" GrantAllRanges="false"
GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="SalesTestAccount2" RangeID="3" GrantAllRanges="false"
GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="QAMasterAdmin" RangeID="4" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="false"/>
    <User UserName="SalesTravellingTestAccount" RangeID="" GrantAllRanges="false"
GrantAnyIP="true" DenyAccess="false"/>
    <User UserName="Bob" RangeID="" GrantAllRanges="true" GrantAnyIP="false"
DenyAccess="false"/>
    <User UserName="Sally" RangeID="" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="true"/>
  </UserMapping>
</AccessRules>
```

```
</UserMapping>  
</AccessRules>
```

## Web Links - Inbound and Outbound

Aside from API operations described later in the document, the KServer also supports the following inbound and outbound links:

### Inbound

The URL to display the **Machine Summary** web page for a specific machine ID is:

```
http://...?machName=<MachineID>
```

For example:

```
http://demo.kaseya.com?machName=jconners.acme
```

The screenshot shows a web browser window displaying the 'Machine Summary' page for a machine named 'morpheus.unnamed'. The page has a blue header with a 'Close' button and a 'HELP' icon. Below the header is a navigation menu with tabs for 'Machine Info', 'Installed Applications', 'System Info', 'Disk Volumes', 'PCI & Disk Hardware', 'Printers', 'Pending Scripts', 'Agent Logs', 'Alerts', 'Patch Status', 'Remote Control', and 'Agent Settings'. The main content area is divided into three sections: 'Computer Information', 'Network Information', and 'Time Information'. The 'Computer Information' section lists details such as Computer Name (morpheus), OS (XP), Version (Professional Edition Service Pack 2 Build 2600), RAM (1023MB), and CPU (1) 1993 MHz Intel(R) Pentium(R) 4 CPU 2.00GHz, Model 2 Stepping 4. The 'Network Information' section lists IP Address (192.168.240.101), Subnet Mask (255.255.255.0), Default Gateway (192.168.240.1), Connection Gateway (66.218.38.45), MAC Address (00-08-A1-03-48-5A), DHCP Server (192.168.240.1), DNS Server (66.51.205.100 - 66.51.206.100), and Primary WINS (WINS disabled). The 'Time Information' section shows KServer time (local) and Agent time (local) as 5:49:46 pm 25-Oct-07. The footer of the page reads 'Powered by Kaseya - Copyright © 2000-2007 Kaseya. All rights reserved.'

Computer Information	
Computer Name:	morpheus
OS:	XP
Version:	Professional Edition Service Pack 2 Build 2600
RAM:	1023MB
CPU:	(1) 1993 MHz Intel(R) Pentium(R) 4 CPU 2.00GHz, Model 2 Stepping 4

Network Information	
IP Address:	192.168.240.101
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.240.1
Connection Gateway:	66.218.38.45
MAC Address:	00-08-A1-03-48-5A
DHCP Server:	192.168.240.1
DNS Server:	66.51.205.100 - 66.51.206.100
Primary WINS:	WINS disabled
Secondary WINS:	

Time Information	
KServer time (local):	5:49:46 pm 25-Oct-07
Agent time (local):	5:49:46 pm 25-Oct-07

## API Web Services

The URL to display the **Ticket** web page for a specific ticket ID is:

`http://...?tucid=<TicketID>`

For example:

`http://demo.kaseya.com?tucid=1234`

The screenshot shows a web form for a ticket with ID 1041. At the top, there is a 'Ticket ID' field containing '1041' and an 'Associate ticket with' dropdown menu showing 'mt-ws002 unnamed'. Below this is a 'Summary' field with the text 'mt-ws002 unnamed has 10.6% free space left'. The form is divided into two main sections: 'Submitter Information' and a list of ticket details. The 'Submitter Information' section includes fields for Name, Email, and Phone, along with an 'Update' button. The ticket details section includes dropdown menus for Assignee (set to '< unassigned >'), Category (set to 'Workstation configuration'), Status (set to 'Open'), Priority (set to 'High'), SLA Type (set to 'None'), Dispatch Tech (set to 'Yes'), Approval (set to 'Not required'), On site (set to 'Yes'), Warranty Work (set to 'Yes'), Billable (set to 'Yes'), Hardware type (set to 'Laptop'), and Blood type (set to 'ab-'). There is also a text input for 'Number of Siblings' set to '0'. At the bottom of the form, there are checkboxes for 'Enter new note' and 'Suppress email notifications'. Below the form is a table of notes with columns for 'Time/Admin', 'Note', and 'Hide'. A single note is visible, dated '7:33:49 pm 12-Oct-07', with the text 'D: on mt-ws002 unnamed has 12356MB free space (10.6%) on a 115718MB disk drive' and a '\*Alert\*' tag.

## Outbound

To customize **New Ticket** links on the **Live Connect** page, fill out the `externalLink.xml` file as described in the comments section of the XML below. To activate the new ticket link, place the `externalLink.xml` file in the `\WebPages\install\` directory of your KServer.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
  machineNameVal - the machine name for the active machine is substituted
  in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
  url="http://192.168.212.52/?mname=machineNameVal&gname=groupNameVal"/>
</externalLinks>
```

## VSA API Web Service - Operations

The following operations can be performed using the **VSA API Web Service**.

### AddMachGroupToScope

Adds a machine by `GroupName` to `ScopeName`.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AddOrg**

Adds an organization.

A single record of the following fields is returned.

orgOutId	decimal	The organization ID of the newly added organization.
orgOutRef	string	The fully qualified name of the organization. Uses dot notation if parent or child organizations exists. Examples: <ul style="list-style-type: none"> <li>▪ neworgname</li> <li>▪ parentorgname.neworgname</li> <li>▪ parentorgname.childorgname.neworgname</li> </ul>
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AddOrgDeptStaff**

Adds a staff member to the department of an organization.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AddOrgToScope**

Adds an organization to a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AddScope**

Adds a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **AddScopeOrg**

Adds an organization and a scope in one pass and associates the organization to the scope.

A single record of the following fields is returned.

orgOutRef	string	The fully qualified name of the organization. Uses dot notation if parent or child organizations exists. Examples: <ul style="list-style-type: none"> <li>neworgname</li> <li>parentorgname.neworgname</li> <li>parentorgname.childorgname.neworgname</li> </ul>
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **AddTicRequest**

Adds a provisional TicketRequest.

A single record of the following fields is returned.

newId	string	Unique identifier.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **AddUserToRole**

Add a user to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **AddUserToScope**

Add a user to a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AdminGroupAccess**

Assigns a machine group to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AssignRole**

Assigns or removes a user to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **AssignScope**

Assigns or removes a user to a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **Authenticate**

Required to begin the VSA API Web Service session. The SessionID returned must be submitted with every method invoked during session. The SessionID is only valid when received from the same machine the authentication originates from.

A single record of the following fields is returned.

SessionID	decimal	The unique session ID assigned to a user connection with the target URL.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.

## API Web Services

ErrorLocation	string	If blank, no error was returned.
---------------	--------	----------------------------------

### Automatic Logon During Authentication

When you authenticate through the API, you are automatically logged into VSA as well. If you are already logged into the VSA at authentication time, the 2 sessions are synchronized. Either way, the result is the same – you end up with valid sessions in both worlds.

The VSA looks for the API's 26 digit SessionID on the query string of every VSA page. So, if the application developer needs to redirect to a VSA page, he can now get directly to a page without forcing the user to log in again. The syntax is:

URL?apiLogonGuid=12345678901234567890123456

For example:

http://someServer:123/Systemtab/SomePage?apiLogonGuid=12345678901234567890123456&SomeVar=Some Value

API activity keeps the VSA session alive. However, since VSA does not assume there is always a need for an API session, VSA activity does not keep the API session alive.

The API uses the same timeout value as the VSA, which is maintained using the VSA's System > [Logon Policy](#) (page 425) page, and has a system default value of 30 minutes.

### AuthenticateWithAppSessionID

Gets API SessionID from a valid AppSession. Only available from local server.

A single record of the following fields is returned.

SessionID	decimal	The unique session ID assigned to a user connection with the target URL.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

**Note:** See [Authenticate](#) (page 525) to initiate a new session.

### CloseAlarm

Closes the alarm for the submitted MonitorAlarmID. Within the VSA user interface, alarms are closed manually using the Monitor > [Alarm Summary](#) (page 198) page.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### CreateAdmin

Creates a VSA user. The password must be hashed.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.

ErrorLocation	string	If blank, no error was returned.
---------------	--------	----------------------------------

### **CreateAgentInstallPackage**

Creates an agent installation package.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **CreateMachineGroup**

Creates a machine group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **CreateRole**

Creates a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteAdmin**

Deletes the specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteAgent**

Deletes the agent on the target machine and corresponding machine ID account in the VSA.

A single record of the following fields is returned.

## API Web Services

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteAgentInstallPackage**

Deletes an agent install package.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteMachineGroup**

Deletes the specified machine group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteOrg**

Deletes the specified organization.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteRole**

Deletes the specified user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## DeleteScope

Deletes the specified scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## DisableAdmin

Disables a specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## Echo

Test method for connectivity test and benchmarking. Does not require authentication. Returns the submitted string.

A single record of the following field is returned.

EchoResult	string	This value should match the input included in the request.
------------	--------	--

## EchoMt

Test method for connectivity test and benchmarking into the middle-tier. Requires authentication. Returns the submitted string. Returns back (echoes) the submitted payload string.

A single record of the following fields is returned.

Payload	string	The string submitted with the request.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## EnableAdmin

Enables a specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.

ErrorLocation	string	If blank, no error was returned.
---------------	--------	----------------------------------

## GetAlarm

Returns alarm detail for the submitted MonitorAlarmID.

A single record of the following fields is returned.

Machine_GroupID	string	A concatenated representation of the machine id and the group ID it is associated with
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	string	Machine Name used for each agent
GroupName	string	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	int	0 - Counter 1 - Service 2 - Process 3 - SNMP 4 - Alert - Alerts are further classified using <a href="#">alert types</a> (page 586). 5 - System Check 6 - EPS 7 - Log Monitoring
AlarmType	string	0 - Alarm 1 - Trending
Message	string	Message created from alarm, email message body
AlarmSubject	string	Subject of alarm and email subject
AlarmEmail	string	Email Address(es) alarm is sent to
EventTime	string	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
AdminName	string	User who assigned monitor counter to machine
MonitorName	string	Name of monitor SNMP Get object
LogType		1 - Application Log 2 - Security Log 3 - System Log
EventType	int	1 - Error 2 - Warning 4 - Informational 8 - Success Audit 16 - Failure Audit
LogValue	decimal	Value causing alarm, if the return value of the SNMP Object Get command is a string the value will be the the Message
SNMPName	string	Name returned from SNMP Device on scan
SNMPCustomerName	string	Custom name for SNMP Device
SystemCheckParam1	string	First parameter used in system check
SystemCheckParam2	string	(Optional) Second parameter used by system check
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetAlarmList

Returns an array of new alarms added since last request by default. Returns all alarms when ReturnAllRecords is set to true.

Multiple records of the following fields are returned, if applicable.

Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
MonitorAlarmID	int	unique monitor alarm number
AlertType	int	Alerts are one of several <b>monitor types</b> (page 594). 1 - Admin account disabled 2 - Get File change alert 3 - New Agent checked in for the first time 4 - Application has been installed or deleted 5 - Agent Procedure failure detected 6 - NT Event Log error detected 7 - KServer stopped 8 - Protection violation detected. 9 - PCI configuration has been changed 10 - Disk drive configuration change 11 - RAM size changed. 12 - Test email sent by serverInfo.asp 13 - Scheduled report completed 14 - LAN Watch alert type 15 - agent offline 16 - low on disk space 17 - disabled remote control 18 - agent online 19 - new patch found 20 - patch path missing 21 - patch install failed 23 - Backup Alert
AlarmSubject	string	Subject of alarm and email subject
EventTime	dateTime	Date and time of alarm

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetGroupLicenseInfo

Gets the allowed number of seats for the specified group.

A single record of the following fields is returned.

MaxAgents	int	The maximum number of agents that can be installed for this machine group.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.

ErrorLocation	string	If blank, no error was returned.
---------------	--------	----------------------------------

## GetLogEntry

Returns transaction log detail for the submitted TransactionID.

A single record of the following fields is returned.

LogTransactionId	decimal	The log transactionID.
LogErrorLocation	string	The log error location.
LogErrorMessage	string	The log error message.
LogMethod	string	The log operation that requested a response.
ExecutionTimeInSeconds	decimal	The log time required to respond to the request.
SessionId	decimal	The log session ID.
UserName	string	The log user name.
ClientIP	string	The log IP address of the client.
DateSubmitted	dateTime	The log date and time the request was submitted.
DateUpdated	dateTime	The log date and time the response was returned.
TransactionXML	string	The XML message used to submit the request.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetMachine

Returns machine detail for the submitted Machine\_GroupID.

A single record of the following fields is returned.

Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
machName	string	full machine name. Everything to the left of the left-most decimal point is the machine name.
groupName	string	full group name for this account. Everything to the right of the left most decimal point is the group name.
Manufacturer	string	Manufacturer string (type 1)
ProductName	string	Product Name string (type 1)
MachineVersion	string	Version string (type 1)
SysSerialNumber	string	Serial Number string (type 1)
ChassisSerialNumber	string	Chassis Serial Number (type 3)
ChassisAssetTag	string	Chassis Asset Tag number (type 3)
BusSpeed	string	External Bus Speed (in MHz) (type 4)
MaxMemorySize	string	Maximum Memory Module Size (in MB) (type 16 - Maximum Capacity or if type 16 not available, Maximum Memory Module Size type 5)

MaxMemorySlots	string	Number of Associated Memory Slots (Number of Memory Devices in type 16 or if type 16 not available Number of Associated Memory Slots in type 5)
ChassisManufacturer	string	Chassis Manufacturer (type 3)
ChassisType	string	Chassis Type (type 3)
ChassisVersion	string	Chassis Ver (type 3)
MotherboardManufacturer	string	Motherboard Manufacturer (type 2)
MotherboardProductCode	string	Motherboard Product Code (type 2)
MotherboardVersion	string	Motherboard Version (type 2)
MotherboardSerialNumber	string	Motherboard Serial Number (type 2)
ComputerName	string	Name of the Computer
IpAddress	string	IP Address of the computer in a.b.c.d notation
SubnetMask	string	Subnet mask in a.b.c.d notation. String is empty if data is unavailable
DefaultGateway	string	Default gateway IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer1	string	DNS server #1s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer2	string	DNS server #2s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer3	string	DNS server #3s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer4	string	DNS server #4s IP address in a.b.c.d notation. String is empty if data is unavailable.
DhcpEnabled	int	0 -> Data is unavailable, 1 -> DHCP on client computer is enabled, 2 -> Disabled
DhcpServer	string	DHCP servers IP address in a.b.c.d notation. String is empty if data is unavailable.
WinsEnabled	string	0 -> Data is unavailable, 1 -> WINS resolution on client computer is enabled, 2 -> Disabled
PrimaryWinsServer	string	Primary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
SecondaryWinsServer	int	Secondary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
ConnectionGatewayIp	int	IP Address in a.b.c.d notation obtained by the Kserver as the source address of the Agent. This IP is the Agents network gateway and will be different from the IpAddress if the computer is behind NAT for example. String is empty if unavailable.
OsType	string	String contains OS type, such as NT4, 2000, NT3.51, or WIN32s. Derived from portions of MajorVersion, MinorVersion, and PlatformId.
OsInfo	string	String contains additional OS info, such as Build 1381 Service Pack 3. Derived from portions of BuildNumber and CsdVersion.
MajorVersion	decimal	Major version number from GetVersionEx() Windows function call.
MinorVersion	string	Minor version number from GetVersionEx() Windows function call. If PlatformId is Win32 for Windows, then a 0 MinorVersion indicates Windows 95. If PlatformId is Win32 for Windows, then then a MinorVersion > 0 indicates Windows 98.
MacAddr	string	String containing the physical address, i.e. the Media Access Control address, of the connection. A MAC address has the form of: 00-03-47-12-65-77

## API Web Services

LoginName	string	User name of the currently logged on user. This value is updated with every quick check in. The agent error log file is updated with each change.
firstCheckin	dateTime	timestamp recording the first time this agent checked into the system
lastCheckin	dateTime	timestamp recording the most recent time this agent checked into the system
currentUser	string	login name of the currently logged in user. Blank if no one logged in at this time
lastLoginName	string	login name of the last user to log into this system
lastReboot	dateTime	timestamp when this system was last rebooted
agentVersion	int	version number of agent installed on this system
contactName	string	User contact name assigned to this agent
contactEmail	string	User email address assigned to this agent
contactPhone	string	User email address assigned to this agent
contactNotes	string	Notes associated with the contact information for this agent
enableTickets	int	0 if this user does not have access to ticketing through the user interface
enableRemoteControl	int	0 if this user does not have access to remote control through the user interface
enableChat	int	0 if this user does not have access to chat through the user interface
credentialName	string	The username of the credential set for this agent (if any)
primaryKServer	string	address:port agent connects to for its primary kserver connection
secondaryKServer	string	address:port agent connects to for its secondary kserver connection
quickCheckinSecs	int	the time to wait, in secs, before performing another agent quick check-in
agentTempDir	string	The working directory used by the agent on this system

Multiple records of the following fields are returned, if applicable.

CpuDesc	string	CPU description (e.g. Pentium III Model 8)
CpuSpeed	int	CPU speed in MHz (e.g. 601)
CpuCount	int	Number of processors (e.g. 1)
TotalRam	int	Amount of RAM in MBytes (e.g. 250)

Multiple records of the following fields are returned, if applicable.

DriveLetter	string	Logical disk drive letter (e.g. C)
TotalSpace	int	Total MBytes on the disk (e.g. 28609 for 28.609 GB) May be null if unavailable.
UsedSpace	int	Number of MBytes used (e.g. 21406 for 21.406 GB). May be null if unavailable.
FreeSpace	int	Number of MBytes free (e.g. 21406 for 21.406 GB). May be null if unavailable.
DriveType	string	Fixed = hard diskRemovable = floppy or other removable mediaCDROMNetwork = mapped network drive
VolumeName	string	Name assigned to the volume
FormatType	string	NTFS, FAT32, CDFS, etc.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
--------	--------	---

TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## ***GetMachineCollectionList***

Returns an array of all machine collections. Items returned can be used as arguments on GetMachineList to filter output.

Multiple records of the following field are returned, if applicable.

collectionName	string	The name of the collection.
----------------	--------	-----------------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## ***GetMachineGroupList***

Returns an array of all MachineGroups the authenticated account has privileges to see. Items returned can be used as arguments on GetMachineList to filter output.

Multiple records of the following field are returned, if applicable.

groupName	string	The machine group ID.
-----------	--------	-----------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## ***GetMachineList***

Returns an array of all the machines that the authenticated user has access rights to see. Supports optional filtering of the return by submitted MachineGroup or MachineCollection. Multiple records of the following fields are returned, if applicable.

Multiple records of the following fields are returned, if applicable.

MachineGroupID	string	A currently existing Machine group. If this field is left blank all machines will be returned.
IpAddress	string	the IP address of the agent machine
MacAddr	string	the MAC address of the agent machine
groupName	string	Group Name used for each agent
firstCheckin	datetime	the first time an agent checks into the VSA
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetMachineUptime

Returns an array of machine uptime statistics for a submitted `AgentGuid` or `MachineGroup` or all machines when `ReturnAllRecords` is set to true. `rptDate` sets the starting sample date of the calculation to current.

All outputs are subjected to security filtering, including the `agentGuid` singleton and `MachineGroup` sub grouping. So if you submit an `agentGuid` or `MachineGroup` you do not have permissions to view, you will get nothing back.

Multiple records of the following field are returned, if applicable.

agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
machineName	string	Full machine name. Everything to the left of the left-most decimal point is the machine name.
totalOnline	int	Total seconds system was online across the measurement time.
measureTime	int	Total seconds system was measured (latest - oldest - suspend alarm times).
latestStatDate	dateTime	Latest time the system was measured, usually the last agent log entry for an offline system.
olderStatDate	dateTime	Earliest time system was measured.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetNotesList

Returns an array of new ticket notes added since last request. Generates a maximum of 500 records in date order and records the most recent note output. User can just keep executing this method until no records are returned.

- `AddedSince` - Including this date in the request overrides the system default "since last read" behavior.

Multiple records of the following fields are returned, if applicable.

TicketID	int	The ticket ID.
Author	string	The author of the note.
DateEntered	dateTime	The date the note was created or last modified.
NoteText	string	The text of the note.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.

ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetOrgLocation

Returns an organization's street address, including its longitude and latitude.

A single record of the following fields is returned.

orgId	string	Unique identifier.
orgRef	string	Unique name.
partitionId	string	Tenant identifier.
orgName	string	The name of the organization.
street	string	The street address.
city	string	The city.
usState	string	The state.
postalCode	string	The zip code.
country	string	The country.
countryCode	string	The country code.
longitude	string	The longitude of the organization location.
latitude	string	The latitude of the organization's location.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetOrgs

Returns the organizations the logged on VSA user can access.

Multiple records of the following field are returned, if applicable.

orgName	string	The organization's name.
orgRef	string	Unique name.
orgID	string	Unique identifier.
CustomerID	string	Unique customer identifier.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetOrgsByScopeID

Returns the organizations a specified scope can access.

## API Web Services

Multiple records of the following field are returned, if applicable.

orgName	string	The organization's name.
orgRef	string	Unique name.
orgID	string	Unique identifier.
CustomerID	string	Unique customer identifier.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetOrgTypes

Returns machine detail for the submitted Machine\_GroupID.

Multiple records of the following fields are returned.

orgTypeID	decimal	Unique identifier.
orgTypeRef	string	The unique name of the organization type.
status	int	1=Active
description	string	A description of the organization type.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetPackageURLs

Gets a list of all agent deploy package URLs available to the logged on user.

Multiple records of the following fields are returned, if applicable.

URL	string	The URL.
PackageName	string	The agent deploy package name.
Description	string	The description of the agent deploy package.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetPartnerUserLocation

Returns the the location of a tenant-specific VSA user, including the VSA user's longitude and latitude.

A single record of the following fields is returned.

adminId	string	The VSA user's unique identifier.
adminName	string	The VSA user's name.
partitionId	string	The tenant identifier.
longitude	string	The longitude of the VSA user's location.
latitude	string	The latitude of the VSA user's location.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetPublishedViewColumns

Returns an array of all columns for a published database view.

Multiple records of the following fields are returned.

name	string	Name of the database view column.
dataType	string	Datatype of the database view column.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## Example

**Note:** The following example was executed using the test page published with every installation, located at <http://localhost/vsaWS/testClient/testClient.asp>.

### Request

```
<req>
  <viewName>vScriptLog</viewName>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```

### Response

```
<GetPublishedViewColumnsResponse>
  <GetPublishedViewColumnsResult>
    <PublishedViewColumns>
      <PublishedViewColumn>
        <name>AdminName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>agentGuid</name>
        <dataType>numeric(26,0)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>EventTime</name>
        <dataType>datetime</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>groupName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
    </PublishedViewColumns>
  </GetPublishedViewColumnsResult>
</GetPublishedViewColumnsResponse>
```

```

    <PublishedViewColumn>
      <name>Machine_GroupID</name>
      <dataType>varchar(201)</dataType>
    </PublishedViewColumn>
    <PublishedViewColumn>
      <name>machName</name>
      <dataType>varchar(100)</dataType>
    </PublishedViewColumn>
    <PublishedViewColumn>
      <name>ScriptDesc</name>
      <dataType>varchar(1000)</dataType>
    </PublishedViewColumn>
    <PublishedViewColumn>
      <name>ScriptName</name>
      <dataType>varchar(260)</dataType>
    </PublishedViewColumn>
  </PublishedViewColumns>
</Method>GetPublishedViewColumns</Method>
<TransactionID>3</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetPublishedViewColumnsResult>
</GetPublishedViewColumnsResponse>

```

## GetPublishedViewRows

Returns an array of all rows for a published database view given a WHERE clause.

A single record of the following fields is returned.

PublishedViewRows	string	Array of row data.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## Example

**Note:** The following example was executed using the test page published with every installation, located at <http://localhost/vsaWS/testClient/testClient.asp>.

## Request

```

<req>
  <viewName>vScriptLog</viewName>

  <columnsList>AdminName,agentGuid,EventTime,Machine_GroupID,ScriptDesc,ScriptName</columnsList>
  <whereClause>EventTime > DATEADD(hour,4,getdate())</whereClause>
  <orderByList>agentGuid,EventTime</orderByList>
  <ReturnAllRows>>false</ReturnAllRows>
  <SessionID>42131527423841487151422001</SessionID>
</req>

```

## SQL Equivalent

```

select top 5000 AdminName,agentGuid,EventTime,Machine_GroupID,ScriptDesc,ScriptName
from vScriptLog
where EventTime > DATEADD(hour,-4,getdate())
order by agentGuid,EventTime

```

Selects 6 of 8 available columns from vScriptLog where activity occurred within the past 4 hours and sorts the results by machine, then activity date.

**Note:** When `<ReturnAllRows>` is set false, a rowset maximum of 5000 is applied to protect the database from overly large resultsets.

## Response

```
<GetPublishedViewRowsResponse>
  <GetPublishedViewRowsResult>
    <PublishedViewRows>
      <vScriptLog>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:1905:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>KES Update AVG via Internet</ScriptName>
        </Row>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:20.00305:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>KES Update</ScriptName>
        </Row>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:20.00705:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>Run Now KES Update</ScriptName>
        </Row>
      </vScriptLog>
    </PublishedViewRows>
  <Method>GetPublishedViewRows</Method>
  <TransactionID>4</TransactionID>
  <ErrorMessage/>
  <ErrorLocation/>
</GetPublishedViewRowsResult>
</GetPublishedViewRowsResponse>
```

## GetPublishedViews

Returns an array of all published database views.

Multiple records of the following fields are returned.

PublishedView	string	Name of the database view.
---------------	--------	----------------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## Example

**Note:** The following example was executed using the test page published with every installation, located at <http://localhost/vsaWS/testClient/testClient.asp>.

Usage details for each view in this list are published in [Database Views](#) (page 477) in the online help and the user guide. There may be more total views documented than the list published via the API.

## API Web Services

### Request

```
<req>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```

### Response

```
<GetPublishedViewsResponse>
  <GetPublishedViewsResult>
    <PublishedViews>
      <PublishedView>
        <viewName>vAddRemoveList</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAdminNotesLog</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAgentConfiguration</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAgentLabel</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAlertLog</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBackupLog</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBaseApplicationInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBaseCpuInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBaseDiskInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBaseDriveManufacturer</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBasePciInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vBasePrinterInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCollectionMember</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vConfigLog</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCurrApplicationInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCurrCpuInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCurrDiskInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCurrDriveManufacturer</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCurrPciInfo</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vCurrPrinterInfo</viewName>
      </PublishedView>
      <PublishedView>
    </PublishedView>
  </GetPublishedViewsResult>
</GetPublishedViewsResponse>
```

```
<viewName>vEventDetail</viewName>
</PublishedView>
<PublishedView>
  <viewName>vEventInstanceDetail</viewName>
</PublishedView>
<PublishedView>
  <viewName>vEventInstanceHistoryDetail</viewName>
</PublishedView>
<PublishedView>
  <viewName>vkadComputers</viewName>
</PublishedView>
<PublishedView>
  <viewName>vkadUsers</viewName>
</PublishedView>
<PublishedView>
  <viewName>vLicenseInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMachine</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMonitorAlarmAlert</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMonitorAlarmCounter</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMonitorAlarmProcess</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMonitorAlarmService</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMonitorAlarmSNMP</viewName>
</PublishedView>
<PublishedView>
  <viewName>vMonitorAlarmSystemCheck</viewName>
</PublishedView>
<PublishedView>
  <viewName>vNetStatsLog</viewName>
</PublishedView>
<PublishedView>
  <viewName>vNtEventLogs</viewName>
</PublishedView>
<PublishedView>
  <viewName>vOnBoardDeviceInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vPatchApprovalStatus</viewName>
</PublishedView>
<PublishedView>
  <viewName>vPatchPolicy</viewName>
</PublishedView>
<PublishedView>
  <viewName>vPatchPolicyMember</viewName>
</PublishedView>
<PublishedView>
  <viewName>vPatchStatus</viewName>
</PublishedView>
<PublishedView>
  <viewName>vPortInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vScriptLog</viewName>
</PublishedView>
<PublishedView>
  <viewName>vScriptStatus</viewName>
</PublishedView>
<PublishedView>
  <viewName>vSystemInfo</viewName>
</PublishedView>
```

## API Web Services

```
<PublishedView>
  <viewName>vTicketField</viewName>
</PublishedView>
<PublishedView>
  <viewName>vTicketNote</viewName>
</PublishedView>
<PublishedView>
  <viewName>vTicketSummary</viewName>
</PublishedView>
<PublishedView>
  <viewName>vUptimeHistory</viewName>
</PublishedView>
<PublishedView>
  <viewName>vProAssetDetails</viewName>
</PublishedView>
</PublishedViews>
<Method>GetPublishedViews</Method>
<TransactionID>2</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetPublishedViewsResult>
</GetPublishedViewsResponse>
```

### GetRoles

Returns the roles the logged on VSA user can access.

Multiple records of the following field are returned, if applicable.

roleID	string	Unique identifier
isActive	boolean	Role is active or inactive.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetScopes

Returns the scopes the logged on VSA user can access.

Multiple records of the following field are returned, if applicable.

scopeID	string	Unique identifier.
---------	--------	--------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetSessionDetails

Gets Session details from either a submitted AppSessionID or valid API SessionID. AppSessionID variant only available from local server.

A single record of the following fields is returned.

adminId	int	VSA user identifier
---------	-----	---------------------

partitionId	decimal	partition identifier
machineIdFil	string	session value of machine filter
activeViewId	int	session value of machine view
groupIdFil	string	session value of group filter
rowPerPage	int	session value of rows per page
startRow	int	starting position in result set
sortField	string	current data document sort field
sortOrder	int	current data document sort order
RoleId	int	role identifier
AdminRole	string	the name of the role
ScopeId	decimal	scope identifier
AdminScope	string	the name of the scope
AppSessionExpiration	dateTime	expiration of session
adminName	string	VSA user name
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetTicket

Returns ticket detail for the submitted MonitorTicketID.

TicketID	int	unique trouble ticket ID number
Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
machName	string	Machine Name used for each agent
groupName	string	Group Name used for each agent
TicketSummary	string	summary string briefly describing the ticket
Assignee	string	Admin name this ticket is assigned to
CreatedBy	string	admin name (or machine ID if entered by user) of the person that created this ticket
CreationDate	string	timestamp when the ticket was created
DueDate	string	ticket due date
LastModifiedDate	string	Date of the most recent note entered for this ticket
ResolutionDate	string	timestamp when the ticket was closed
UserName	string	The name of the submitter
UserEmail	string	The email address of the submitter
UserPhone	string	The phone number of the submitter

Multiple records of the following fields are returned, if applicable.

TicketLabel	string	The label of the field
IntegerValue	int	The value of a integer field

NumberValue	decimal	The value of a number field
StringValue	string	The value of a string field
ListValue	string	The value of a list field

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetTicketList

Returns an array of new tickets added since last request by default. Returns all tickets when ReturnAllRecords is set to true.

Multiple records of the following fields are returned, if applicable.

TicketID	int	unique trouble ticket ID number
Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
TicketSummary	string	summary string briefly describing the ticket

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetTicketNotes

Returns an array of notes belonging to the submitted ticket.

Multiple records of the following fields are returned, if applicable.

TicketID	int	The ticket ID.
Author	string	The author of the note.
DateEntered	dateTime	The date the note was created or last modified.
NoteText	string	The text of the note.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **GetTicRequestTicket**

Returns the ticketID associated with a ticket request ID.

A single record of the following fields is returned.

ticketId	string	unique identifier for ticket
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **GetVerboseMachineGroupList**

Multiple records of the following field are returned, if applicable.

groupName	string	The machine group ID.
machGroupGuid	string	GUID of the machine group.
parentGroupGuid	string	GUID of the parent machine group, in one exists.
orgFK	string	Foreign key to the organization containing the machine group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **LockFunctionAccess**

Locks function access of the submitted user role to the submitted base user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **Primitives**

The following primitive Datatype operations are also provided. Each primitive operation uses the same xml contract as their corresponding multiple-columns operation. Each primitive returns a string value that requires subsequent processing.

<b>Primitive</b>	<b>Result</b>	<b>Datatype</b>
PrimitiveAddMachGroupToScope	PrimitiveAddMachGroupToScopeResult	string
PrimitiveAddOrg	PrimitiveAddOrgResult	string
PrimitiveAddOrgDeptStaff	PrimitiveAddOrgDeptStaffResult	string
PrimitiveAddOrgToScope	PrimitiveAddOrgToScopeResult	string

## API Web Services

PrimitiveAddScope	PrimitiveAddScopeResult	string
PrimitiveAddScopeOrg	PrimitiveAddScopeOrgResult	string
PrimitiveAddTicRequest	PrimitiveAddTicRequestResult	string
PrimitiveAddUserToRole	PrimitiveAddUserToRoleResult	string
PrimitiveAddUserToScope	PrimitiveAddUserToScopeResult	string
PrimitiveAssignRole	PrimitiveAssignRoleResult	string
PrimitiveAssignScope	PrimitiveAssignScopeResult	string
PrimitiveAuthenticate	PrimitiveAuthenticateResult	string
PrimitiveCloseAlarm	PrimitiveCloseAlarmResult	string
PrimitiveCreateMachineGroup	PrimitiveCreateMachineGroupResult	string
PrimitiveCreateRole	PrimitiveCreateRoleResult	string
PrimitiveDeleteMachineGroup	PrimitiveDeleteMachineGroupResult	string
PrimitiveDeleteOrg	PrimitiveDeleteOrgResult	string
PrimitiveDeleteScope	PrimitiveDeleteScopeResult	string
PrimitiveEchoMt	PrimitiveEchoMtResult	string
PrimitiveGetAlarm	PrimitiveGetAlarmResult	string
PrimitiveGetAlarmList	PrimitiveGetAlarmResult	string
PrimitiveGetLogEntry	PrimitiveGetLogEntryResult	string
PrimitiveGetMachine	PrimitiveGetMachineResult	string
PrimitiveGetMachineCollectionList	PrimitiveGetMachineCollectionListResult	string
PrimitiveGetMachineGroupList	PrimitiveGetMachineGroupListResult	string
PrimitiveGetMachineGroups	PrimitiveGetMachineGroupsResult	string
PrimitiveGetMachineList	PrimitiveGetMachineListResult	string
PrimitiveGetMachineUptime	PrimitiveGetMachineUptimeResult	string
PrimitiveGetNotesList	PrimitiveGetNotesListResult	string
PrimitiveGetOrgLocation	PrimitiveGetOrgLocationResult	string
PrimitiveGetOrgs	PrimitiveGetOrgsResult	string
PrimitiveGetOrgsByScopeID	PrimitiveGetOrgsByScopeIDResult	string
PrimitiveGetOrgTypes	PrimitiveGetOrgTypesResult	string
PrimitiveGetPartnerUserLocation	PrimitiveGetPartnerUserLocationResult	string
PrimitiveGetPublishedViewColumns	PrimitiveGetPublishedViewColumnsResult	string
PrimitiveGetPublishedViewRows	PrimitiveGetPublishedViewRowsResult	string
PrimitiveGetPublishedViews	PrimitiveGetPublishedViewsResult	string
PrimitiveGetRoles	PrimitiveGetRolesResult	string
PrimitiveGetScopes	PrimitiveGetScopesResult	string
PrimitiveGetTicRequestTicket	PrimitiveGetTicRequestTicketResult	string
PrimitiveGetTicket	PrimitiveGetTicketResult	string
PrimitiveGetTicketList	PrimitiveGetTicketListResult	string
PrimitiveGetTicketNotes	PrimitiveGetTicketNotesResult	string
PrimitiveGetVerboseMachineGroup List	PrimitiveGetVerboseMachineGroupListResult	string
PrimitiveRemoveUserFromRole	PrimitiveRemoveUserFromRoleResult	string
PrimitiveResetPassword	PrimitiveResetPasswordResult	string

PrimitiveSetPartnerUserLocation	PrimitiveSetPartnerUserLocationResult	string
PrimitiveUpdateOrg	PrimitiveUpdateOrgResult	string
PrimitiveUpdateTicket	PrimitiveUpdateTicketResult	string
PrimitiveUpdateUser	PrimitiveUpdateUserResult	string

## ***RemoveUserFromRole***

Removes a VSA user from a role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## ***ResetPassword***

Resets the specified user's password.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## ***RoleMembership***

Assigns a user to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## ***SendAdminMessage***

Send a message to a user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## SetAdminPassword

Resets the password for a specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## SetGroupLicenseInfo

Sets the maximum number of agents allowed for a specified group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## SetPartnerUserLocation

Sets the current longitude and latitude of the VSA user

A single record of the following fields is returned.

AdminId	decimal	Unique identifier of the VSA user.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## UpdateOrg

Updates the information for an organization.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## UpdateTicket

Updates one or more fields of a ticket. Only fields listed on the Ticketing > [Email Reader](#) (page 449) page can be updated.

## Updating List Fields

In the example below the `Origin` field is a `List` type field with four possible values. A request passes the name of the field, `Origin`, and a number representing the position of the value in the list, *counting from 1*. For example, the value `Phone` is in the second position in the list, so the value passed to change the `Origin` field to `Phone` is `2`.

**Warning:** Changing the order of field drop-down list values by re-sequencing them or by entering a new value in the middle of the list will change the value selected by the `UpdateTicket` operation. Ensure users are aware of this integration constraint before changes are made to `Email Reader` field values.

Define ticketing fields and default values		
Field Label	Type	Default Value
Status	List	Under Investigation
Category	List	Support Request
Priority	List	2-Normal
Customer ID	String	
Forum	List	No Article Applies
Feature	List	Core - Agent Tab
Origin	List	Email
Related Tickets	String	Email
Current Tier	List	Manually Entered
Resolution	List	Web Site
		< Edit List >
		<not resolved>

Update    New

## Closing a Ticket

Updating a ticket can include closing a submitted `MonitorTicketID` by updating the `Status` field with a value of `3`, which represents the third value in the `Status` field drop-down list. An example is shown below. Additional `<TicketField>` name/value elements could be added to the example below to update multiple fields.

```
<UpdateTicketRequest>
  <TicketID>1</TicketID>
  <TicketFields>
    <TicketField>
      <Name>Status</Name>
      <Value>3</Value>
    </TicketField>
  </TicketFields>
  <SessionID>13642146236194247244181221</SessionID>
</UpdateTicketRequest>
```

## Updating Other Types of Fields

The following other types of ticket fields can be updated:

- `String` - Can contain any text up to 500 characters in length. Best used to hold things like problem location or other variables that do not belong in the summary line.
- `Integer` - Can contain any positive or negative integer value.
- `Number (nn.d)` - A number that always shows one digit to the right of the decimal point.
- `Number (nn.dd)` - A number that always shows two digits to the right of the decimal point.
- `Number (nn.ddd)` - A number that always shows three digits to the right of the decimal point.
- `Number (nn.dddd)` - A number that always shows four digits to the right of the decimal point.
- `AddNote` - Adds a plain text note to the specified ticket.
- `HideNote` - Sets hidden property to the note being added.

## API Web Services

Fields being modified by the fields array write a hidden audit note to the ticket specified with field name, old value and new value. For example, ~API~ [CR] Status has changed from Open to Closed.

### Returned Fields

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### Ticket Attachments

The API Web Service cannot be used to get or update ticket file attachments. Ticket file attachments are typically located in C:\Kaseya\WebPages\ManagedFiles directory of the KServer. API developers are responsible for writing code to place attachment files in this directory before making Web Service API calls that reference these attachments.

### UpdateUser

Updates user information.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

---

## Agent Procedure API Web Service

### In This Section

Enabling the Agent Procedure API Web Service	552
Agent Procedure API Web Service - Operations	552

### Enabling the Agent Procedure API Web Service

See the [VSA API Web Service](#) (page 513) online help or user guide for a general introduction to the Kaseya API.

To enable the Agent Procedure API Web Service:

- Display the System > Configure page in the VSA.
- Check the [Enable VSA API Web Service](#) checkbox.
- Access the Agent Procedure API web service using `http://<your-KServer>/vsaWS/AgentProcWS.asmx`

### Agent Procedure API Web Service - Operations

The following operations can be performed using the [Agent Procedure API Web Service](#).

## AddScriptAssignment

Adds a scriptAssignment row to perform a RunNow script execution. The authenticated user must have view access to the script and the current role must be allowed the Enable Scheduling function. A single record of the following field is returned.

ScriptAssignmentId	int	A unique identifier for a row in the scriptAssignmentTable, representing the combination of an agentGUID and a scriptID.
--------------------	-----	--

## AddScriptPrompt

Adds agent procedure prompt variables to an agent procedure. Scripts that prompt for variables at schedule time store the values in a table. These variables are unique for each scheduled instance of the script (not the script). This allows different people to schedule the same script using different variable values. The authenticated user must have view access to the agent procedure to which prompts are being added.

A single record of the following field is returned.

AddScriptPromptResult		There is no response other than an error message, if applicable.
-----------------------	--	--

## Echo

Test Method for connectivity test and benchmarking. Does not require Authentication. Returns the submitted string.

A single record of the following field is returned.

Echo	string	This value should match the input included in the request.
------	--------	--

## EchoMt

Test method for connectivity test and benchmarking into the middle-tier. Requires authentication. Returns the submitted string. Returns back (echoes) the submitted payload string.

A single record of the following fields is returned.

Payload	string	The string submitted with the request.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetScriptAssignmentId

Gets the scriptAssignmentId for a scriptId/agentGuid combination.

A single record of the following field is returned.

ScriptAssignmentId	int	A unique identifier for a row in the scriptAssignmentTable, representing the combination of an agentGUID and a scriptID.
--------------------	-----	--

## GetScriptIdFromScriptName

Returns an array of script objects with basic information about all scripts with the requests name. Only scripts with view access for the authenticated user are returned.

A single record of the following fields are returned.

ScriptId	int	Unique identifier of the script.
ScriptName	string	Name of the script.
TreePath	string	Location of the script in the folder tree.

---

## Monitoring API Web Service

### In This Section

Enabling the Monitoring API Web Service	554
Monitoring API Web Service - Operations	554

## Enabling the Monitoring API Web Service

See the [VSA API Web Service](#) (page 513) online help or user guide for a general introduction to the Kaseya API.

To enable the Monitoring API Web Service:

- Display the System > Configure page in the VSA.
- Check the [Enable VSA API Web Service](#) checkbox.
- Access the Monitoring API web service using `http://<your-KServer>/vsaWS/monitoringWS.asmx`

## Monitoring API Web Service - Operations

The following operations can be performed using the [Monitoring API Web Service](#).

### AssignEventAlertToMachine

Assigns an event alert to a machine.

A single record of the following fields is returned.

NewId	int	A unique identifier of the event alert.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### AssignEventLogMachineSettings

Assigns event log settings to a machine.

A single record of the following fields is returned.

NewId	int	A unique identifier of the event log setting assignment.
Method	string	The operation that requested this response.

TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **CreateEventSet**

Create a new event set. Returns the new event set ID.

A single record of the following fields is returned.

NewId	int	A unique identifier of the new event set.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **CreateEventSetDefinition**

Creates an event set definition.

A single record of the following fields is returned.

NewId	int	A unique identifier of the new event set definition.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteAllEventAlertsFromMachine**

Deletes all event alerts assigned to a machine.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **DeleteAllEventLogMachineSettings**

Deletes all windows event log machine settings assigned to a machine.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

**DeleteEventAlertFromMachine**

Deletes specific event alert from machine, by event log type and category.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

**DeleteEventLogMachineSettings**

Deletes windows event log machine settings assigned to a machine, by event log type.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

**DeleteEventSet**

Deletes an event set and all of its definitions.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

**DeleteEventSetDefinition**

Deletes an event set definition by event set definition ID.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

**GetEventAlertList**

Gets alert events assigned to a machine.

Multiple records of the following fields are returned.

AgentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
AlertEmail	string	Email addresses an alert email is sent to.

EventLogTypeid	int	Unique id number associated with this event log. For example: Application -> 796450521 DNS Server -> 1208407329 Security -> 1664713117 System -> 1380569194  When the event log type is pulled from a windows machine, if it doesn't exist it will be created in this table with a unique Id. This Id will be the same across all systems, this is accomplished by using the name in the creation of the Id.
EventLogCategoryValue	int	1 - Error 2 - Warning 4 - Informational 8 - Success Audit 16 - Failure Audit 256 - Critical 512 - Verbose
EventSetId	int	A unique identifier of the event set.
AgentProcedureId	int	Unique identifier of agent procedure to run if an alert is created. 0 or null = do not run a script
AgentProcedureMachGuid	decimal	The unique identifier of the machine the agent procedure is run on.
CreateTicket	boolean	If true, a ticket is created if an alert is created.
SendEmail	boolean	If true, email is sent if an alert is created.
CreateAlarm	boolean	If true, an alarm is created if an alert is created.
CriteriaType	int	The criteria to meet to trigger an alert. 0, null = single event 1 = multiple events for duration 2 = missing event for duration.
EventCount	int	Number of events to occur before an alert is triggered
AlarmDurationSecs	int	Number of seconds to wait before an alert is triggered.
AlarmRearmSec	int	Number of seconds to wait after an alert has occurred before a new alert is triggered for the same criteria.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## **GetEventLogMachineSettingsList**

Returns event log settings for a specific machine.

Multiple records of the following fields are returned.

MachineName	string	Full machine name. Everything to the left of the left most decimal point is the machine name.
AgentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.

## API Web Services

EventLogTypeId	int	Unique id number associated with this event log. For example: Application -> 796450521 DNS Server -> 1208407329 Security -> 1664713117 System -> 1380569194  When the event log type is pulled from a windows machine, if it doesn't exist it will be created in this table with a unique Id. This Id will be the same across all systems, this is accomplished by using the name in the creation of the Id.
EventLogName	string	The event log type name.
EventAssignValue	int	Value determining the types of events to pull from the event log. Stored as a bitmap with the following weights: 1 – error 2 – warning 4 – info 8 – success audit 16 – failure audit 256 – critical 512 – verbose

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **GetEventSetDefinitionList**

Returns an event set definition.

Multiple records of the following fields are returned.

EventSetId	int	A unique identifier of the event set.
Ignore	int	0,null – to apply these filter settings using LIKE 1 – to apply these filter settings using NOT LIKE
Source	string	Filter used to match the event log source field.
Category	string	Filter used to match the event log category field.
EventId	int	Filter used to match the event log event ID field.
UserName	string	Filter used to match the event log username field.
Description	string	Filter used to match the event log description field.
EventSetDefId	int	A unique identifier of the event set definition.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### **GetEventSetList**

Returns a list of event sets.

Multiple records of the following fields are returned.

SetName	string	The name of the event set.
EventSetId	int	A unique identifier of the event set.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## KSD API Web Service

### In This Section

Enabling KSD API Web Service	559
KSD API Web Service Data Types	559
KSD API Web Service - Operations	566
Sample Messages	569

### Enabling KSD API Web Service

See the VSA API Web Service online help or user guide for a general introduction to the Kaseya API.

To enable the KSD API Web Service:

- Display the System > Configure page in the VSA.
- Check the [Enable VSA API Web Service](#) checkbox.
- Access the KSD API web service using `http://<your-KServer>/vsaWS/vsaServiceDeskWS.asmx`

### KSD API Web Service Data Types

The following are the major data types used in the [KSD API Web Service](#). These data types are defined in the XML schema document in the `XML\Schemas\ServiceDesk\ServiceDeskDefinition.xsd` file located in the directory where the Kaseya software is installed.

**Note:** In the descriptions that follow, where the name says (content) that means the value is the content of the element.

#### Legend

- A - AddIncident
- G - GetIncident
- L - ListIncidents
- U - UpdateIncident

### RefItem

The [RefItem](#) describes an item that is a reference item in the service desk. These have an internal database ID value, an internal name, an optional description and the display value.

G	ref	string	The internal name of the item. This is usually prefixed by the service
---	-----	--------	--

## API Web Services

			desk name and     , such as Standard     Open.
G	id	string	The internal database key for the item.
G	description	string	The optional description for the item.
G	(content)	string	The user readable form of the item.

## CustomField

The **CustomField** describes the value of a custom field in an incident.

AGU	fieldName	string	The name of the field within the service desk.
AGU	(content)	string	The value of the custom field.

## Note

The **Note** describes a single note attached to a ticket.

G	User	string	The name of the user that created the note.
G	Timestamp	dateTime	The time the note was created.
AG	Text	string	The content of the note. This may be HTML formatted, and may include references to attachments.
AG	Hidden	boolean	True if the note should be hidden.
AG	HoursWorked	Decimal	The number of hours worked in this update of the ticket.
AG	SuppressNotify	Boolean	True if notifications for this update should be suppressed.

## Attachment

The **Attachment** describes a single attachment for the ticket.

A	Name	string	A unique identifying string for this attachment.
A	DisplayName	string	The name of the attachment as seen by the user.
A	FileName	string	The original name of the file or URL.
A	DocumentType	string	The MIME format of the attachment.
A	Content	Base64Binary	The base 64 encoded content for the attachment.

## RelatedIncident

The **RelatedIncident** is another incident that has been related to this current incident

AGU	IncidentNumber	string	The unique identifier for the incident.
G	Summary	string	The summary of the related incident.
G	Status	string	The user readable status of the related incident.
G	Description	string	The description field of the incident.

## ServiceDeskDefinition

The following **ServiceDeskDefinition** elements returned describe the desk definition used to edit the ticket. This provides each of the possible values for each field in the ticket.

A single record of the following elements returned.

ServiceDeskDefinition	id="decimal"	A unique identifier.
Name	string	The name of the desk definition.
Description	string	A brief description of the desk definition.
RequireTime	boolean	If true, entering hours worked is required.
DisplayMachineInfo	boolean	If true, machine lookup field is displayed.
RequireMachineInfo	boolean	If true, machine lookup association is required.
DisplayOrgInfo	boolean	If true, organization lookup field is displayed.
RequireOrgInfo	boolean	If true, organization lookup association is required.
DisplayCI	boolean	obsolete
RequireCI	boolean	obsolete
AllAdmins	boolean	obsolete
AutoStartClock	boolean	If true, a clock is automatically started when the user starts to edit the ticket.
AutoSaveClock	boolean	If true, when the ticket is saved, the difference between the current time and the start time is entered as the Hours Worked.
AutoInsertNote	boolean	If true, notes are automatically added to each ticket for the changes made to the ticket.
AutoInsertNoteHidden	boolean	If true, automatically generated notes are made hidden.
NeedStatusNote	boolean	obsolete
SDPrefix	string	The prefix code added to the beginning of the ticket ID.
DefaultStatus	decimal	Default status value. Refers to one of the elements with the matching id attribute in the Status section.
DefaultStage	decimal	Default stage value. Refers to one of the elements with the matching id attribute in the Stage section.
DefaultPriority	decimal	Default priority value. Refers to one of the elements with the matching id attribute in the Priority section.
DefaultSeverity	decimal	Default severity value. Refers to one of the elements with the matching id attribute in the Severity section.
DefaultResolution	decimal	Default resolution value. Refers to one of the elements with the matching id attribute in the Resolution section.
DefaultCategory	decimal	Default category value. Refers to one of the elements with the matching id attribute in the Category section.
DefaultSubCategory	decimal	Obsolete
DefaultServiceDesk	boolean	If true, this is the default service desk, the first one selected when creating new tickets.
TemplateName	string	The template file used to initially create the service desk. Not used otherwise.
TemplateType	int	The type of service desk: 1=ticket, 3=knowledge base.
SequenceName	string	For internal development use only.
EditingTemplate	string	The name of the form used to edit tickets for the service desk.
ShowNotesPane	boolean	If true, notes pane displays in lower pane of Tickets table.

## API Web Services

ShowWorkOrders	boolean	If true, display work order and work order line in ticket editor.
ShowSessionTimers	boolean	If true, display session timers in ticket editor.
ShowTasks	boolean	If true, display tasks tab and task related fields.
EstimatedHours	double	Total number of hours worked estimated to resolve this ticket.
ActualHours	double	Total number of hours entered to resolve this ticket.
EmailReader	string	The email reader associated with the service desk.
Administrator	string	The user that is the "desk administrator" of the service desk. The desk administrator is notified of certain errors within the service desk.
DefaultPolicy	string	The default policy assigned to the desk.
Status	RefItem	Returns a list of child elements of each Status value in the service desk.
Priority	RefItem	Returns a list of child elements of each Priority value in the service desk.
Severity	RefItem	Returns a list of child elements of each Severity value in the service desk.
Resolution	RefItem	Returns a list of child elements of each Resolution value in the service desk.
TaskStatus	RefItem	Returns a list of child elements of each TaskStatus value in the service desk.
Categories	RefItem	Returns a list of child elements of each Category value in the service desk. Each Category can include child SubCategory elements if they exist.
Stages		Returns a list of child elements of each Stage value in the service desk. Each Stage is identified by a Begin, Middle, or End stagetype attribute. Each stage has the following child elements: <ul style="list-style-type: none"> <li>• Item - The name of the stage.</li> <li>• Initialization - The Stage Entry procedure linked to the stage.</li> <li>• Escalation - The Escalation procedure linked to the stage. Time and Units are specified as attributes.</li> <li>• Goal - The Goal linked to the stage. The Goal procedure linked to the stage. Time and Units are specified as attributes.</li> <li>• NextStage – One of the next stages that this stage may transition to.</li> </ul>
Participants	RefItem	The list of users as pools that may be assignees or owners for the service desk.
CurrentContact		Contact information about the user logged on during this transaction. If the user is associated with a staff record, then the <code>CurrentContact</code> information is culled from the staff record. If the currently logged on user is a machine user using <a href="#">Portal Access</a> , then <code>CurrentContact</code> information is culled from the Home > Change Profile tab of <a href="#">Portal Access</a> . <ul style="list-style-type: none"> <li>• ContactName</li> <li>• PhoneNumber</li> <li>• Organization</li> <li>• EmailAddress</li> </ul>
SubmitterTypes	string	Type of person submitting the ticket: <ul style="list-style-type: none"> <li>• UNKNOWN</li> <li>• PARTICIPANT - A participant is a VSA user.</li> <li>• USER - Someone not known to VSA.</li> </ul>

CustomFields		Returns zero or more Field elements, each with the following hierarchy: <ul style="list-style-type: none"> <li>• Caption - Screen caption.</li> <li>• Title - Report title.</li> <li>• Fieldname - Name of the field.</li> <li>• FieldFormat - Data type.</li> <li>• DefaultValue - Default value, if a List data type.</li> <li>• Values - collection element, if a List data type.</li> </ul> <small>Item - List item value.</small>
AccessRights		Returns a hierarchy of child elements: <ul style="list-style-type: none"> <li>• ViewHiddenNotes - true or false</li> <li>• ChangeHiddenNotes - true or false</li> <li>• Field Rights&gt;Field Right - collection elements</li> </ul> <small>FieldName - Name of the ticket field AccessType - Required, Edit, View Only, Hidden</small>
NoteTemplates		Returns a list of note templates, each representing standard text that can be added to ticket notes.
ChangeProcedure	string	The Change Ticket procedure associated with the service desk.
GoalProcedure	decimal	The Goal procedure associated with the service desk. <ul style="list-style-type: none"> <li>• time – the amount of time for goal</li> <li>• unit – The units of time</li> <li>• (content) – the name of the goal procedure.</li> </ul>
ResourceTypes		The list of resource types that can be assigned to a ticket.
TaskDefinitions		The list of task values that can be assigned to a task status.
AssocPolicies		The list of policies that can be associated with a ticket.

## Incident Summary

The [IncidentSummary](#) contains the basic description of a ticket.

AGLU	ServiceDeskName	string	The name of the desk definition.
GLU	IncidentNumber	string	The ticket identifier.
AGLU	Summary	string	The ticket summary text.
AGLU	Description	string	The ticket description. text.
AGLU	Status	string	The ref status of the ticket.
AGLU	Priority	string	The ref priority of the ticket.
AGLU	Resolution	string	The ref resolution type of the ticket.
AGLU	Stage	string	The ref stage of the ticket.
AGLU	Severity	string	The ref severity of the ticket.
AGLU	Category	string	The ref category of the ticket.
AGLU	SubCategory	string	The ref subcategory of the ticket.
GL	Policy	string	The policy of the ticket.
GL	CreateDateTime	dateTime	The date time the ticket was created.
GL	LastEditDateTime	dateTime	The date time the ticket was last edited.
GL	CloseDateTime	dateTime	The date time the ticket was closed.
AGLU	OrgID	decimal	Unique identifier of the organization associated with the ticket.
AGLU	OrganizationName	string	The organization name associated with the ticket.

## API Web Services

AGLU	Organization	string	The organization ID associated with the ticket.
AGLU	OrganizationStaffName	string	The organization staff member name associated with the ticket.
AGLU	OrganizationStaff	string	The organization staff member unique ID associated with the ticket.
AGLU	OrganizationStaffEmail	string	The email of the organization staff member associated with the ticket.
AGLU	Machine	string	The machine associated with the ticket.
AGLU	MachineGuid	decimal	The GUID of the machine associated with the ticket.
AGLU	MachineGroup	string	The machine group of the machine associated with the ticket.
AGLU	MachineGroupGuid	decimal	The GUID of the machine group associated with the the ticket.
AGLU	Submitter	string	The name of the submitter who submitted the ticket.
AGLU	SubmitterEmail	string	The email of the ticket submitter.
AGLU	SubmitterPhone	string	The phone of the ticket submitter.
AGLU	SubmitterType	string	Type of person submitting the ticket: <ul style="list-style-type: none"> <li>• UNKNOWN</li> <li>• PARTICIPANT - A participant is a VSA user.</li> <li>• USER - Someone not known to VSA.</li> </ul>
GL	IsUnread	boolean	If true, the ticket has not been viewed by the currently logged on user.

## Incident

The **Incident** is derived from the **IncidentSummary** and contains all of the fields of the **IncidentSummary** in addition to these fields.

G	IsParticipant	boolean	obsolete
G	IsClosed	boolean	True if closed.
G	CurrentStageEscalationDateTime	dateTime	Stage escalation date and time.
G	CurrentGoalDateTime	dateTime	Stage goal date and time.
AGU	Owner	string	Owner of the ticket.
	Participant	string	obsolete
AGU	AssigneeType	string	Type of assignee: <ul style="list-style-type: none"> <li>• UNKNOWN</li> <li>• PARTICIPANT - individual assignee</li> <li>• POOL - a pool of users</li> </ul>
AGU	Assignee	string	Assignee name.
AGU	AssigneeEmail	string	Assignee email.
G	ActualCompletionDate	dateTime	obsolete
G	ExpectedCompletionDate	dateTime	Date time the ticket is or was expected to be closed, (the ticket goal due date).
G	ActualResolutionDate	dateTime	Date time a resolution type was set for the ticket.
AGU	PromisedDate	dateTime	Date time promise date entered by the customer representative to resolve the ticket.
G	IsArchived	boolean	True if ticket is archived.
G	IsError	boolean	obsolete
G	IsPoolAssignee	boolean	obsolete

	ErrorMessage	string	obsolete
	Notify	boolean	obsolete
G	CurrentStage	string	The current stage.
AGU	ResolutionNote	string	Descriptive text entered with the resolution type.
G	LockTime	dateTime	Date time the ticket was locked by opening the ticket for editing.
G	LockUser	string	User locking the ticket by opening the ticket for editing.
G	StageGoalTime Remaining	int	The time remaining before the stage goal timer executes the goal procedure. Rrelevant when the stage goal has been paused.
AGU	SourceType	string	The source type, either a system event or email, that generated a ticket request. <ul style="list-style-type: none"> <li>• Email</li> <li>• Backup</li> <li>• KES</li> <li>• Patch</li> <li>• Monitor</li> <li>• Alarm</li> <li>• Portal</li> <li>• ServiceDesk</li> <li>• Other</li> </ul>
	OrgAddress/Address	string	Org address 1
	OrgAddress/Address	string	Org address 2
	OrgAddress/City	string	Org city
	OrgAddress/State	string	Org state
	OrgAddress/Zip	string	Org zip
	OrgAddress/Country	string	Org address
AGLU	Field	CustomField	Zero or more custom fields values
AGU	Notes	Note	Zero or more notes.
AGU	Attachments	Attachment	Zero or more attachments
AGU	RelatedIncidents	Related Incident	Zero or more related incidents
	StartDate	datetime	start date/time of the task
	EndDate	datetime	end date/time of the task
	UpdateTime	datetime	last date/time this task was updated
	FollowupDate	datetime	date/time to followup on this task
	CompletionDate	datetime	completion date/time of this task
	ApprovalDate	datetime	approval date/time of this task
	PromiseDate	datetime	promise date/time for this task
	PercentCompletion	int	percent completion of this task
	TaskStatus	string	status of this task
	ActualHours	double	total hours worked for this task
	Resource	Resource	Zero or more resources
	Assignee	string	assignee assigned to this task

## API Web Services

	EstimatedHours	decimal	Estimated total hours worked for this ticket.
	TotalHours	decimal	Actual hours worked for this ticket.
	PreviousStage	string	PreviousStage of this ticket.
	WorkPerformedDateTim e	datetime	Datetime work was performed on this ticket.
	EditingTemplate	string	Editing template used to edit this ticket.
GU	ServiceDeskDefinition	ServiceDesk Definition	

## KSD API Web Service - Operations

The following operations can be performed using the [KSD API Web Service](#).

### AddIncident

The request is:

AddSDIncident	Incident	The content of the new incident to create. Only fields marked with an A in the first column can be set.
SessionId	Decimal	The web service session ID.

A single record of the following fields is returned.

IncidentNumber	string	The unique identifier of the ticket.
IncidentID	decimal	The identifier of the ticket.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### AddServDeskToScope

The request is:

servDeskName	string	The name of the service desk.
scopeName	string	The name of the scope.
SessionId	decimal	The web service session ID.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

### GetIncident

Retrieves a single incident from the database. The request is:

IncidentRequest		The incident to retrieve. This has the following fields: <ul style="list-style-type: none"> <li>• IncidentNumber – The ticket ID as seen by the user, such as STD000001</li> <li>• IncidentId – The database ID of the ticket to retrieve.</li> <li>• IncludeNotes – true to include notes in the retrieved ticket</li> <li>• IncludeDefinition – true to include the desk definition in the response</li> </ul>
SessionId	Decimal	The web service session ID.

A single record of the following fields is returned.

IncidentResponse	Incident	The retrieved incident.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetIncidentList

Retrieve a list of incidents matching the request criteria. The request is:

IncidentRequest		The incident to retrieve. This has the following fields: <ul style="list-style-type: none"> <li>• ServiceDeskName – The name of the service desk to query.</li> <li>• Status – One or more status values to match. If no status values are supplied, then tickets are retrieved regardless of status.</li> <li>• Priority – One or more priority values to match. If no priority values are supplied, then tickets are retrieved regardless of priority.</li> <li>• Stage – One or more stage values to match. If no stage values are supplied, then tickets are retrieved regardless of stage.</li> <li>• Summary – a string or expression to search the summary of tickets.</li> <li>• Organization – The name or partial name of organizations to match. If not supplied, then tickets are retrieved for all organizations within the scope.</li> <li>• OrganizationStaff – The name of an organizational staff member. associated with tickets. If not supplied, then tickets are retrieved for all organizations within the scope.</li> <li>• Machine – The name of a machine to match. If not supplied, then tickets are retrieved for all machines within the scope.</li> <li>• MachineGroup – The name of a machine group to match. If not supplied, then tickets are retrieved for all machine groups within the scope.</li> <li>• Assignee – The name or partial name of assignees to match. If not supplied, then tickets are retrieved for all assignees within scope.</li> <li>• StartingIncident – When paging, this is the next incident number to retrieve. This value comes from the nextStartingIncident value of a previous GetIncidentList request.</li> <li>• IncidentCount – When present, specifies the number of</li> </ul>
-----------------	--	---

## API Web Services

		incidents to retrieve. <ul style="list-style-type: none"> <li>SortField – When present, sorts the results on the field name.</li> </ul>
SessionId	Decimal	The web service session ID.

The response is the following:

IncidentList		The list of matching incidents. This has the following attributes and elements: <ul style="list-style-type: none"> <li>totalIncidents – The total number of incidents that match the request.</li> <li>nextStartingIncident – the Id of the next incident to retrieve.</li> <li>Incident – zero or more incident matching the request criteria.</li> </ul>
SessionId	Decimal	The web service session ID.

## GetServiceDesk

Retrieves the definition of a service desk. This should be called prior to creating a user interface to allow the user to enter a ticket. The request is:

ServiceDeskDefinitionRequest		The service desk to retrieve. This has the following elements: <ul style="list-style-type: none"> <li>ServiceDeskName – The name of the service desk to retrieve.</li> <li>ServiceDeskID – the database of the service desk to retrieve. Should not be used.</li> </ul>
SessionId	Decimal	The web service session ID.

A single record of the following elements returned.

ServiceDeskDefinitionResponse	ServiceDeskDefinition	The retrieved desk definition.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## GetServiceDesks

Multiple records of the following fields are returned, if applicable. The request is:

IsDefault	boolean	If true, the service desk is the default service desk.
ServiceDeskID	decimal	A unique identifier.
ServiceDeskName	string	The name of the service desk.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## Primitives

The following primitive Datatype operations are also provided. Each primitive operation uses the same xml contract as their corresponding multiple-columns operation. Each primitive returns a string value that requires subsequent processing. You are strongly discouraged from using these methods.

Primitive	Result	Datatype
PrimitiveAddIncident	PrimitiveAddIncidentResult	string
PrimitiveAddServDeskToScope	PrimitiveAddServDeskToScopeResult	string
PrimitiveGetIncident	PrimitiveGetIncidentResult	string
PrimitiveGetIncidentList	PrimitiveGetIncidentListResult	string
PrimitiveGetServiceDesk	PrimitiveGetServiceDeskResult	string
PrimitiveGetServiceDesks	PrimitiveGetServiceDesksResult	string
PrimitiveUpdateIncident	PrimitiveUpdateIncidentResult	string

## UpdateIncident

Updates a single incident in the database. The request is:

UpdateSDIncident	Incident	The incident to update. See the first column of the Incident data type for the fields that are valid on update.
SessionId	Decimal	The web service session ID.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

## Sample Messages

Sample data is included in the following XMLs.

### GetServiceDesks Request

```
<GetServiceDesks xmlns="vsaServiceDeskWS">
  <req>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetServiceDesks>
```

### GetServiceDesks Response

```
<GetServiceDesksResponse xmlns="vsaServiceDeskWS">
  <GetServiceDesksResult>
    <ServiceDesks>
      <ServiceDesk>
        <IsDefault>>false</IsDefault>
        <ServiceDeskID>291273277175176</ServiceDeskID>
        <ServiceDeskName>KnowledgeBase</ServiceDeskName>
      </ServiceDesk>
    </ServiceDesks>
  </GetServiceDesksResult>
</GetServiceDesksResponse>
```

## API Web Services

```
<IsDefault>>false</IsDefault>
<ServiceDeskID>696191121914314</ServiceDeskID>
<ServiceDeskName>Standard</ServiceDeskName>
</ServiceDesk>
</ServiceDesks>
<Method>GetServiceDesks</Method>
<TransactionID>144</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetServiceDesksResult>
</GetServiceDesksResponse>
```

## GetServiceDesk Request

```
<GetServiceDesk xmlns="vsaServiceDeskWS">
  <req>
    <ServiceDeskDefinitionRequest>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName
>
      <ServiceDeskID
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">696191121914314</ServiceD
eskID>
    </ServiceDeskDefinitionRequest>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetServiceDesk>
```

## GetServiceDesk Response

```
<GetServiceDeskResponse xmlns="vsaServiceDeskWS">
  <GetServiceDeskResult>
    <ServiceDeskDefinitionResponse id="696191121914314">
      <Name
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</Name>
      <Description
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard SD</Description>
      <RequireTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</RequireTime>
      <DisplayMachineInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</DisplayMachineInfo>
      <RequireMachineInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</RequireMachineInfo
>
      <DisplayOrgInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</DisplayOrgInfo>
      <RequireOrgInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</RequireOrgInfo>
      <DisplayCI
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</DisplayCI>
      <RequireCI
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</RequireCI>
      <AllAdmins
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</AllAdmins>
      <AutoStartClock
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</AutoStartClock>
      <AutoSaveClock
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</AutoSaveClock>
      <AutoInsertNote
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</AutoInsertNote>
      <AutoInsertNoteHidden
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</AutoInsertNoteHidde
n>
      <NeedStatusNote
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</NeedStatusNote>
      <SDPrefix
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD</SDPrefix>
      <DefaultStatus
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">218924116119912</DefaultS
tatus>
```

```

    <DefaultStage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">831768438118427</DefaultS
tage>
    <DefaultPriority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">693719171716599</DefaultP
riority>
    <DefaultSeverity
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultSeverity>
    <DefaultResolution
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultResolution>
    <DefaultCategory
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultCategory>
    <DefaultSubCategory
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultSubCategory>
    <DefaultServiceDesk
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</DefaultServiceDesk
>
    <TemplateType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">1</TemplateType>
    <SequenceName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">SEQ129</SequenceName>
    <EditingTemplate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Fixed_Width_Tabbed.xml</E
ditingTemplate>
    <Status xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|AwaitingHardware" id="541491145218711">Awaiting Hardware</Item>
    <Item ref="Standard|AwaitingUserFeedback" id="281767467828324">Awaiting User
Feedback</Item>
    <Item ref="Standard|Closed" id="989295147216226">Closed</Item>
    <Item ref="Standard|Escalated" id="551271771474242">Escalated</Item>
    <Item ref="Standard|Hold" id="172151822788151">Hold</Item>
    <Item ref="Standard|InProgress" id="111313126312233">In Progress</Item>
    <Item ref="Standard|New" id="218924116119912">New</Item>
</Status>
    <Priority xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|CriticalHigh" id="744512181719881">Critical High</Item>
    <Item ref="Standard|High" id="982525519923522">High</Item>
    <Item ref="Standard|Low" id="291721863176342">Low</Item>
    <Item ref="Standard|Medium" id="693719171716599">Medium</Item>
    <Item ref="Standard|Planning" id="176222131631332">Planning</Item>
</Priority>
    <Severity xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|CompanyWide(High)" id="315477225242249">Whole Company
(High)</Item>
    <Item ref="Standard|MultipleUsers(Medium)" id="262164368749722">Multiple users
(Medium)</Item>
    <Item ref="Standard|OneUser(Low)" id="917688316816914">Single User (Low)</Item>
</Severity>
    <Resolution xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|AdviceGiven" id="498162732192611">Advice Given</Item>
    <Item ref="Standard|CannotDuplicate" id="262514419248621">Cannot Duplicate</Item>
    <Item ref="Standard|ClosedbyCustomerRequest" id="525192125718333">Closed by Customer
Request</Item>
    <Item ref="Standard|HardwareReplaced" id="432262321578326">Hardware Replaced</Item>
    <Item ref="Standard|HotFixReleased" id="189239616133249">Hot Fix Released</Item>
    <Item ref="Standard|InstallationCompleted" id="139764799836252">Installation
Completed</Item>
    <Item ref="Standard|NewSoftwareInstalled" id="521637923418319">New Software
Installed</Item>
    <Item ref="Standard|Noresponsefromuser" id="115424612244857">No response from
user</Item>
    <Item ref="Standard|OSReinstalled" id="531617444692623">OS Reinstalled</Item>
    <Item ref="Standard|Other" id="711261961631328">Other</Item>
    <Item ref="Standard|PassedtoSales" id="191482475814123">Passed to Sales</Item>
    <Item ref="Standard|Pendingscriptcleared" id="762515513181192">Pending script
cleared</Item>
    <Item ref="Standard|ReapplySchema" id="525317525441497">Reapply Schema</Item>
    <Item ref="Standard|Reboot" id="832182442825238">Reboot</Item>
    <Item ref="Standard|ResolvedbyCustomer" id="243623591961272">Resolved by
Customer</Item>
    <Item ref="Standard|ResolvedbyTechnition" id="423939164212169">Resolved</Item>

```

## API Web Services

```
<Item ref="Standard||SolvedwithKBarticle" id="272199179212412">Solved with KB
article</Item>
<Item ref="Standard||TrainingGiven" id="622224812237126">Training Given</Item>
</Resolution>
<Categories xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
  <Category>
    <Item ref="Standard||Advice& Guidance" id="161211171768212">Advice &
Guidance</Item>
    <SubCategory ref="Standard||Advice& Guidance||General"
id="561699795215782">General</SubCategory>
  </Category>
  <Category>
    <Item ref="Standard||Kaseya" id="641881726251641">Kaseya</Item>
    <SubCategory ref="Standard||Kaseya||AgentIcon" id="821781865922435">Agent
Icon</SubCategory>
    <SubCategory ref="Standard||Kaseya||Alarm" id="481422361723261">Alarm</SubCategory>
    <SubCategory ref="Standard||Kaseya||ApplicationChanges"
id="525187874623717">Application Changes</SubCategory>
    <SubCategory ref="Standard||Kaseya||Disk" id="919621482151882">Disk</SubCategory>
    <SubCategory ref="Standard||Kaseya||Eventlog"
id="814714713317798">Eventlog</SubCategory>
    <SubCategory ref="Standard||Kaseya||GetFile" id="322618792314914">Get
File</SubCategory>
    <SubCategory ref="Standard||Kaseya||Hardware"
id="176166136238942">Hardware</SubCategory>
    <SubCategory ref="Standard||Kaseya||Lanwatch"
id="214791394922624">Lanwatch</SubCategory>
    <SubCategory ref="Standard||Kaseya||Logon_Admin"
id="943315515116292">Logon_Admin</SubCategory>
    <SubCategory ref="Standard||Kaseya||Logon_User"
id="636613429245187">Logon_User</SubCategory>
    <SubCategory ref="Standard||Kaseya||NewAgent" id="557214511134217">New
Agent</SubCategory>
    <SubCategory ref="Standard||Kaseya||Other" id="631281678197153">Other</SubCategory>
    <SubCategory ref="Standard||Kaseya||PatchManagement" id="462824113621914">Patch
Management</SubCategory>
    <SubCategory ref="Standard||Kaseya||Procedure"
id="274262311559714">Procedure</SubCategory>
    <SubCategory ref="Standard||Kaseya||RCDisabled" id="641624812335116">RC
Disabled</SubCategory>
    <SubCategory ref="Standard||Kaseya||Script"
id="471482131991414">Script</SubCategory>
    <SubCategory ref="Standard||Kaseya||SystemOffline" id="113411182222324">System
Offline</SubCategory>
    <SubCategory ref="Standard||Kaseya||SystemOnline" id="251814418923368">System
Online</SubCategory>
    <SubCategory ref="Standard||Kaseya||Unidentified"
id="617313577253122">Unidentified</SubCategory>
  </Category>
  <Category>
    <Item ref="Standard||Network" id="414766231875111">Network</Item>
    <SubCategory ref="Standard||Network||Connectivity"
id="122145211361321">Connectivity</SubCategory>
    <SubCategory ref="Standard||Network||Design"
id="495611529142242">Design</SubCategory>
    <SubCategory ref="Standard||Network||Firewall"
id="812515316323522">Firewall</SubCategory>
    <SubCategory ref="Standard||Network||Other" id="946227769167531">Other</SubCategory>
    <SubCategory ref="Standard||Network||Performance"
id="941891772111717">Performance</SubCategory>
  </Category>
  <Category>
    <Item ref="Standard||Printer" id="155243642251342">Printer</Item>
    <SubCategory ref="Standard||Printer||Other" id="341431321188813">Other</SubCategory>
    <SubCategory ref="Standard||Printer||PrinterProblem" id="851831547314111">Printer
Problem</SubCategory>
    <SubCategory ref="Standard||Printer||PrinterSetup" id="619395216749723">Printer
Setup</SubCategory>
    <SubCategory ref="Standard||Printer||Toner" id="161984536861723">Toner</SubCategory>
  </Category>
</Category>
```

```

        <Item ref="Standard||ServiceRequest" id="541124124415221">Service Request</Item>
        <SubCategory ref="Standard||ServiceRequest||EquipmentMove"
id="862712311517672">Equipment Move</SubCategory>
        <SubCategory ref="Standard||ServiceRequest||NewLaptop" id="266812518245792">New
Laptop</SubCategory>
        <SubCategory ref="Standard||ServiceRequest||NewServer" id="322872913227349">New
Server</SubCategory>
        <SubCategory ref="Standard||ServiceRequest||NewWorkstation" id="224115236352441">New
Workstation</SubCategory>
    </Category>
</Categories>
<Stages xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Stage stageType="End">
        <Item ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</Item>
        <Initialization>Standard Enters Closed</Initialization>
    </Stage>
    <Stage stageType="Begin">
        <Item ref="Standard||Identified" id="831768438118427" description="New ticket is
received">Identified</Item>
        <Initialization>Standard Enters Identified</Initialization>
        <Escalation time="15" unit="MINUTE">Incident is Escalated</Escalation>
        <Goal time="1" unit="HOURL">Identified Goal</Goal>
        <NextStage ref="Standard||Tier1" id="546812745461511" description="Tier 1
Support">Tier1</NextStage>
    </Stage>
    <Stage stageType="Middle">
        <Item ref="Standard||Tier1" id="546812745461511" description="Tier 1
Support">Tier1</Item>
        <Initialization>Standard Enters Tier1</Initialization>
        <Escalation time="3" unit="HOURL">Incident is Escalated</Escalation>
        <Goal time="2" unit="HOURL">Tier1 Goal</Goal>
        <NextStage ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</NextStage>
        <NextStage ref="Standard||Tier2" id="318527191192719" description="Tier 2 Specialist
Support">Tier2</NextStage>
    </Stage>
    <Stage stageType="Middle">
        <Item ref="Standard||Tier2" id="318527191192719" description="Tier 2 Specialist
Support">Tier2</Item>
        <Initialization>Standard Enters Tier2</Initialization>
        <Escalation time="3" unit="HOURL">Incident is Escalated</Escalation>
        <Goal time="4" unit="HOURL">Tier2 Goal</Goal>
        <NextStage ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</NextStage>
    </Stage>
</Stages>
<Participants xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Participant ref="garyw" id="67511883639135112891416313"
isPool="false">garyw</Participant>
    <Participant ref="jschenck" id="72381729521421633172123416"
isPool="false">jschenck</Participant>
    <Participant ref="NickT" id="96171921315349923924634249"
isPool="false">NickT</Participant>
    <Participant ref="Standard||SupportManager" id="654222596258293"
isPool="true">SupportManager (Pool)</Participant>
    <Participant ref="Standard||Tier1Support" id="352161952139188"
isPool="true">Tier1Support (Pool)</Participant>
    <Participant ref="Standard||Tier2Support" id="921522231318131"
isPool="true">Tier2Support (Pool)</Participant>
</Participants>
<CustomFields xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Field id="221552971661261">
        <Caption>Source</Caption>
        <Title>Source</Title>
        <FieldName>Source</FieldName>
        <FieldFormat>List</FieldFormat>
        <DefaultValue>Call</DefaultValue>
        <Values>
            <Item ref="Call" id="0">Call</Item>
            <Item ref="EMail" id="0">EMail</Item>
        </Values>
    </Field>

```

## API Web Services

```
<Item ref="Text" id="0">Text</Item>
</Values>
</Field>
<Field id="818831117157241">
  <Caption>Urgency</Caption>
  <Title>Urgency</Title>
  <FieldName>Urgency</FieldName>
  <FieldFormat>List</FieldFormat>
  <DefaultValue>Medium</DefaultValue>
  <Values>
    <Item ref="High" id="0">High</Item>
    <Item ref="Low" id="0">Low</Item>
    <Item ref="Medium" id="0">Medium</Item>
  </Values>
</Field>
<Field id="513119818455188">
  <Caption>KB Article created</Caption>
  <Title>KB Article Created</Title>
  <FieldName>KB_Article</FieldName>
  <FieldFormat>List</FieldFormat>
  <DefaultValue>No</DefaultValue>
  <Values>
    <Item ref="No" id="0">No</Item>
    <Item ref="Yes" id="0">Yes</Item>
  </Values>
</Field>
<Field id="291214644251233">
  <Caption>Dept</Caption>
  <Title>Department</Title>
  <FieldName>Dept</FieldName>
  <FieldFormat>List</FieldFormat>
  <DefaultValue>IT</DefaultValue>
  <Values>
    <Item ref="Accounting" id="0">Accounting</Item>
    <Item ref="Accounts Payable" id="0">Accounts Payable</Item>
    <Item ref="Facilities" id="0">Facilities</Item>
    <Item ref="HR" id="0">HR</Item>
    <Item ref="IT" id="0">IT</Item>
    <Item ref="Other" id="0">Other</Item>
    <Item ref="Payroll" id="0">Payroll</Item>
    <Item ref="Sales" id="0">Sales</Item>
    <Item ref="Telecom" id="0">Telecom</Item>
  </Values>
</Field>
</CustomFields>
<AccessRights xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
  <ViewHiddenNotes>true</ViewHiddenNotes>
  <ChangeHiddenNotes>true</ChangeHiddenNotes>
  <FieldRights>
    <FieldRight>
      <FieldName>ID</FieldName>
      <AccessType>Required</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Summary</FieldName>
      <AccessType>Required</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Description</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>CreationDtTm</FieldName>
      <AccessType>ViewOnly</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>SubmitterName</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>SubmitterEmailAddr</FieldName>
```

```
<AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ContactPhone</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>OrgName</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>OrgID</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>StaffID</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ContactEmail</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>MachineID</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>Note</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ClosedDtTm</FieldName>
  <AccessType>ViewOnly</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>PromiseDtTm</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>DueDtTm</FieldName>
  <AccessType>ViewOnly</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ActualCompletedDate</FieldName>
  <AccessType>ViewOnly</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>HiddenNote</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>Owner</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>LockUser</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>EditDtTm</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>current_esc_datetime</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>current_goal_datetime</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
```

```

        <FieldName>lockTime</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>sourceType</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Status</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Priority</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Severity</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Category</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>SubCategory</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Stage</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Resolution</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Assignee</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Source</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Urgency</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>KB_Article</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
        <FieldName>Dept</FieldName>
        <AccessType>Edit</AccessType>
    </FieldRight>
</FieldRights>
</AccessRights>
<NoteTemplates xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="My Note" id="196429316815241">My Note</Item>
    <Item ref="Note 2" id="167218821431219">Second note</Item>
</NoteTemplates>
<ChangeProcedure
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard is
Changed</ChangeProcedure>
    <GoalProcedure time="1" unit="DAY"
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard Goal - All
Stages</GoalProcedure>
</ServiceDeskDefinitionResponse>
<Method>GetServiceDesk</Method>
<TransactionID>146</TransactionID>
<ErrorMessage/>

```

```

    <ErrorLocation/>
  </GetServiceDeskResult>
</GetServiceDeskResponse>

```

## GetIncidentList Request

```

<GetIncidentList xmlns="vsaServiceDeskWS">
  <req>
    <IncidentListRequest>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName
>
      <IncidentCount
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">30</IncidentCount>
    </IncidentListRequest>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetIncidentList>

```

## GetIncidentList Response

```

<GetIncidentListResponse xmlns="vsaServiceDeskWS">
  <GetIncidentListResult>
    <IncidentList>
      <Incident xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <ServiceDeskName>Standard</ServiceDeskName>
        <IncidentNumber>STD000001</IncidentNumber>
        <Summary>Getting Started with Service Desk - PLEASE READ!</Summary>
        <Status>Closed</Status>
        <Priority>Low</Priority>
        <Stage>Closed</Stage>
        <Category>Advice & Guidance</Category>
        <CreateDateTime>2010-02-05T17:07:21.55-08:00</CreateDateTime>
        <LastEditDateTime>2010-02-05T22:59:22.64-08:00</LastEditDateTime>
        <Submitter>Kaseya Support</Submitter>
        <SubmitterEmail>noreply@kaseya.com</SubmitterEmail>
      </Incident>
    </IncidentList>
    <Method>GetIncidentList</Method>
    <TransactionID>147</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetIncidentListResult>
</GetIncidentListResponse>

```

## GetIncident Request

```

<GetIncident xmlns="vsaServiceDeskWS">
  <req>
    <IncidentRequest>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000001</IncidentNumber
>
      <IncludeNotes
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IncludeNotes>
      <IncludeDefinition
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IncludeDefinition>
    </IncidentRequest>
    <SessionID>67223225114316912673490269</SessionID>
  </req>
</GetIncident>

```

## GetIncident Response

```

<GetIncidentResponse xmlns="vsaServiceDeskWS">
  <GetIncidentResult>
    <IncidentResponse id="611922114996841">
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000001</IncidentNumber

```

```

>
  <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Getting
Started with Service Desk - PLEASE READ!</Summary>
  <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <p><strong><span
style='font-size:11.0pt;font-family:"Calibri", "sans-serif";color:blue'>WELCOME TO SERVICE
DESK</span></strong></p><br/>
    Your Service Desk module has been pre-configured with a template-driven Standard service desk,
and a Knowledge Base desk. Only a few short customization steps are required to use these desks
immediately. See <a
href="http://help.kaseya.com/WebHelp/EN/KSD/1000000/index.htm?toc.htm?5982.htm">Getting
Started</a> to quickstart your implementation of Service Desk.
    </p>
  </Description>
  <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Closed</Status>
  <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Low</Priority>
  <Stage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Closed</Stage>
  <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Advice&Guid
ance</Category>
  <CreateDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T17:07:21.55-08
:00</CreateDateTime>
  <LastEditDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T22:59:22.64-08
:00</LastEditDateTime>
  <Submitter xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Kaseya
Support</Submitter>
  <SubmitterEmail
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">noreply@kaseya.com</Submi
tterEmail>
  <SubmitterType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">UNKNOWN</SubmitterType>
  <IsUnread
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IsUnread>
  <IsParticipant
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsParticipant>
  <Owner
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Owner>
  <AssigneeType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">POOL</AssigneeType>
  <Assignee
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Tier1Support</Assignee>
  <ActualCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T22:59:29.28-08
:00</ActualCompletionDate>
  <ExpectedCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-06T17:07:22.283-0
8:00</ExpectedCompletionDate>
  <IsArchived
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsArchived>
  <IsError
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsError>
  <Notify
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</Notify>
  <SourceType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">ServiceDesk</SourceType>
  <CustomFields xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Field fieldName="Source">Text</Field>
    <Field fieldName="Urgency">Low</Field>
    <Field fieldName="KB_Article">No</Field>
    <Field fieldName="Dept">Sales</Field>
  </CustomFields>
  <Notes xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Note id="213494962391116">
      <Timestamp>2010-02-05T22:59:25.127-08:00</Timestamp>
      <Text>Auto Generated Note:<br/>
Ticket Changed<br/>      'currentStageGoalDateTime' cleared<br/></Text>

```

```

    <Hidden>true</Hidden>
  </Note>
  <Note id="356934215185622">
    <User>garyw</User>
    <Timestamp>2010-02-05T17:07:21.55-08:00</Timestamp>
    <Text>Auto Generated Note:&lt;br/&gt;
  </Note>
  </Notes>
</IncidentResponse>
<Method>GetIncident</Method>
<TransactionID>200</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetIncidentResult>
</GetIncidentResponse>

```

## AddIncident Request

```

<AddIncident xmlns="vsaServiceDeskWS">
  <req>
    <AddSDIncident>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName
>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Test Ticket
From Web Service</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">This
ticket was created with the web service.</Description>
      <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||New</Status>
      <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Medium</Priorit
y>
      <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Network</Catego
ry>
      <SubCategory
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Network||Conne
ctivity</SubCategory>
    </AddSDIncident>
    <SessionID>67223225114316912673490269</SessionID>
  </req>
</AddIncident>

```

## AddIncident Response

```

<AddIncidentResponse xmlns="vsaServiceDeskWS">
  <AddIncidentResult>
    <AddSDIncidentResponse>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000002</IncidentNumber
>
      <IncidentID
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">249259141859248</Incident
ID>
    </AddSDIncidentResponse>
    <Method>AddIncident</Method>
    <TransactionID>203</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </AddIncidentResult>
</AddIncidentResponse>

```

## UpdateIncident Request

```

<UpdateIncident xmlns="vsaServiceDeskWS">
  <req>
    <UpdateSDIncident id="249259141859248">

```

## API Web Services

```
<ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName
>
  <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000002</IncidentNumber
>
  <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Test Ticket
From Web Service</Summary>
  <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">This
ticket was created with the web service.</Description>
  <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||InProgress</Sta
tus>
  <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Low</Priority>
  <Stage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Identified</Sta
ge>
  <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Printer</Catego
ry>
  <SubCategory
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Printer||Printe
rProblem</SubCategory>
  <CreateDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:07:31.923-0
8:00</CreateDateTime>
  <LastEditDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:07:31.923-0
8:00</LastEditDateTime>
  <Submitter
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Submitter>
  <SubmitterType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">UNKNOWN</SubmitterType>
  <IsUnread
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IsUnread>
  <IsParticipant
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsParticipant>
  <CurrentStageEscalationDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:22:43.063-0
8:00</CurrentStageEscalationDateTime>
  <CurrentGoalDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T22:07:43.077-0
8:00</CurrentGoalDateTime>
  <Owner
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Owner>
  <AssigneeType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">POOL</AssigneeType>
  <Assignee
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Tier1Support</Assignee>
  <ExpectedCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-11T21:07:43.077-0
8:00</ExpectedCompletionDate>
  <IsArchived
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsArchived>
  <IsError
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsError>
  <Notify
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</Notify>
  <Notes xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Note id="281273717819319">
      <User>garyw</User>
      <Timestamp>2010-03-10T21:07:31.923-08:00</Timestamp>
      <Text>Auto Generated Note:&lt;br/&gt;
Ticket Added&lt;br/&gt;</Text>
      <Hidden>true</Hidden>
    </Note>
  </Notes>
</UpdateSDIncident>
</req>
</UpdateIncident>
```

## **UpdateIncident Response**

```
<UpdateIncidentResponse xmlns="vsaServiceDeskWS">
  <UpdateIncidentResult>
    <Method>UpdateIncident</Method>
    <TransactionID>205</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </UpdateIncidentResult>
</UpdateIncidentResponse>
```

**About Kaseya**

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

# Glossary of Terms

## Active Directory

Active Directory is a directory service used to store information about the network resources across a domain. Its main purpose is to provide central authentication and authorization services for Windows based computers. An Active Directory structure is a hierarchical framework of objects. The objects fall into three broad categories: resources (e.g. printers), services (e.g. email) and users (user accounts and groups). The AD provides information on the objects, organizes the objects, controls access and sets security.

The VSA can reference information stored in Active Directory during a [LAN Watch](#) (page 591). Subsequently, agents can be automatically installed on machines using [View AD Computers](#) (page 65). Using [View AD Users](#) (page 66), agents can be automatically installed on each machine a AD user logs onto. Also the latest user contact information can be extracted from Active Directory and applied to the machine ID an AD user is currently logged onto. This provides VSA users with up-to-date contact information automatically.

## Agent Menu

The set of options that display when the user right-clicks the [agent](#) (page 583) icon  in the [system tray](#) (on page 599) of the managed machine. The agent menu can be [customized](#) (page 73).

## Agent Quick View Window

Hovering the cursor over a check-in icon displays an [agent quick view window](#) immediately. You can launch an agent procedure, view logs or launch [Live Connect](#) from the agent quick view window.

## Agent Settings

To provide both flexibility and automation, the VSA enables you to specify different values for the following types of agent settings on a per machine basis:

- [Credential](#) (page 83)
- [Agent Menu](#) (page 73)
- [Check-in Control](#) (page 75)
- [Working Directory](#) (page 78)
- [Logs](#) (page 35)
- Machine Profile - Refers to settings in Audit > [Edit Profile](#) (page 79).
- [View Collections](#) (page 588)
- [Portal Access](#) (page 81)
- [Remote Control Policy](#) (page 362)
- [Patch Settings](#) (page 595)
- [Patch File Source](#) (page 340)
- [Patch Policy Memberships](#) (page 327)
- Fixed Alerts - These all the alert types on the Monitor > [Alerts](#) (page 219) page except for Event Log alerts and System alerts.
- [Event Log Alerts](#) (page 219)
- [Monitor Sets](#) (page 204)
- [Distribute Files](#) (page 129)
- Protection
- Agent Procedure Schedules

### Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the  agent icon—displays in the system tray of the managed machine. **Agent icons** (page 25) can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** (page 592). Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > **Deploy Agents** (page 39) inside the VSA.
- **Multiple agents** (page 45) can be installed on the same machine, each pointing to a different server.
- A **check-in icon** (page 16) displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the  check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called **Live Connect** (page 17). **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an **agent quick view window** (page 583) immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

### Agents - Linux

Linux agents support the following functions:

- Agent procedures
- Latest audits, baselines audits and system audits
- Remote control and FTP with VNC
- Reset Password
- LAN Watch and Install Agents - See **Installing Linux Agents** (page 47).
- Site Customization - The **Agent Icons** tab now includes a set of icons for Linux agents you can customize.
- Only non-plug-in specific items are accessible via a Linux-based Browser or when browsing to Linux agent machine. This is the following:
- Live Connect - Only non-plug-in specific items are accessible via a Linux-based browser or when browsing to a Linux agent machine. Supported menu options include:
  - Home
  - Agent Data
  - Audit Information
  - Ticketing (or Service Desk Ticketing)
  - Chat
  - Video Chat

See System Requirements.

### Agents - Macintosh

Macintosh agents support the following functions:

- Audits - selected hardware and software attributes

- Agent procedures
- Remote Control
- FTP
- Reset Password
- Task Manager
- Live Connect including Desktop Access.
  - On Mac Leopard (Intel), you can use Desktop Access in Live Connect to remote control a Windows system using Firefox or Safari.
  - On Windows using any of our supported browsers you can use Desktop Access to remote control a Mac Leopard (Intel) system.
  - Does not include a thumbnail preview image of the desktop in Live Connect.
- LAN Watch / Install Agents
- Supported monitoring:
  - SNMP monitoring
  - Process monitoring in monitor sets

See System Requirements.

## Alarm

In graphical displays throughout the VSA, when an **alarm condition** (page 585) exists, the VSA displays, by default, a red traffic light  icon. If no alarm condition exists, a green traffic light icon  displays. These icons can be customized.

Alarms, and **other types of responses** (page 586), are enabled using the following pages:

- Agent > **LAN Watch** (page 56)
- Backup > Backup Alerts
- Monitor > **Alerts** (page 219)
- Monitor > **Assign Monitoring** (page 261)
- Monitor > **SNMP Traps Alert** (page 257)
- Monitor > **Assign SNMP** (page 276)
- Monitor > **System Checks** (page 269)
- Monitor > **Parser Summary** (page 288)
- Monitor > **Assign Parser Sets** (page 297)
- Patch Management > **Patch Alerts** (page 342)
- Remote Control > Offsite Alerts
- Security > Apply Alarm Sets

## Alarm Condition

An alarm condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

## Alarms - Suspending

The **Suspend Alarms** page suppresses **alarms** (page 585) for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms.*

## Alert

Alerts are responses to **alarm conditions** (page 585). This differs from an **audit** (page 587), which simply collects selected data for reference purposes without regard to any criteria.

Alerts have two meanings, generic and specific:

### Generic Alerts

Typically there are four types of alert responses to an alarm condition:

- Create **Alarm**
- Create **Ticket**
- Run Procedure
- **Email Recipients**

Defining an alert sets the **ATSE response code** (page 586) for that machine ID or SNMP device.

Alerts are defined using:

- Monitor > **Alerts** (page 219)
- Monitor > **Assign Monitoring** (page 261)
- Monitor > **Assign SNMP** (page 276)
- Monitor > **System Checks** (page 269)
- Monitor > **Parser Summary** (page 288)
- Monitor > **Assign Parser Sets** (page 297)
- Patch Management > **Patch Alerts** (page 342)
- Remote Control > Offsite Alerts
- Backup > Backup Alerts
- Security > Apply Alarm Sets
- Agent > **LAN Watch** (page 56)

### Specific Alerts

The **Alerts** page enables you to quickly define alerts for typical **alarm conditions** (page 585) found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the `Low Disk` type of alarm displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alarm immediately to any machine ID displayed on the **Alerts** page and specify the response to the alarm.

### Alert Types

Alerts are one of several **monitor types** (page 594).

- 1 - Admin account disabled
- 2 - Get File change alert
- 3 - New Agent checked in for the first time
- 4 - Application has been installed or deleted
- 5 - Agent Procedure failure detected
- 6 - NT Event Log error detected
- 7 - KServer stopped
- 8 - Protection violation detected.
- 9 - PCI configuration has been changed
- 10 - Disk drive configuration change
- 11 - RAM size changed.
- 12 - Test email sent by serverInfo.asp
- 13 - Scheduled report completed
- 14 - LAN Watch alert type
- 15 - agent offline
- 16 - low on disk space
- 17 - disabled remote control
- 18 - agent online
- 19 - new patch found
- 20 - patch path missing
- 21 - patch install failed
- 23 - Backup Alert

## ATSE Response Code

**Creating an alarm** represents one of three ways to notify users of an alarm condition. The other two ways are to **send an email** or to **create a ticket**. In addition, alarm conditions can **run** an agent procedure to automatically respond to the alarm condition. These four types of responses are called the **ATSE response code**. Whether assigned to a machine ID, a group ID, or an SNMP device, the designation indicates which types of responses are active for the alarm condition defined.

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

None of the ATSE responses are required. The alarm condition and the ATSE responses, including no response, is reported in the Info Center > Monitor - **Monitor Action Log** (page 167) report.

The same ATSE design applies to all methods of monitoring provided by the VSA.

## Audit

**Agents** (page 583) can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the KServer so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machine's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > **Reports** (page 149) are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 219) types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**.

## Auto Learn Monitor Sets

You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.

## Backup Sets

All files required for a full backup, including all incremental or differential backups, are saved together in a **backup set**.

## Canonical Name

The primary name for an object in DNS. Each object can also have an unlimited number of aliases.

## Chat

Online **chat** is a text-based, instant messaging system. It is included with the KServer primarily to provide immediate technical support. VSA users can chat with machine users and/or chat with other VSA users currently logged on the same Kserver. VSA users can enable or disable the machine user's

## Glossary of Terms

ability to initiate chat sessions with VSA users. Since Kaseya chats are relayed through the KServer, all chats are protected by the Kaseya 256 bit rolling encryption protocol.

### Check-in Status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 583).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

### Check-in: Full vs. Quick

A **full check-in** occurs when an agent completes the processing of any and all outstanding tasks assigned to it by the KServer. These tasks can include processing an agent procedure, posting cached log data, or refreshing the agent configuration file. A full check-in occurs if 24 hours elapses without a specific task requiring it. A **quick check-in** occurs when an account checks in at the configured check-in interval, indicating to the KServer that the managed machine is still online. This doesn't require the completion of all outstanding tasks. Some functions require a full check-in before an agent can begin processing a new task. For example, System > [Naming Policy](#) (page 395). You can force a full check-in by right-clicking the agent icon in the system tray of a managed machine and clicking the [Refresh](#) option.

### Collection

Collections are a free-form selection of *individual machine IDs within a view*. It doesn't matter which groups the machine IDs belong to, so long as the VSA user is authorized to have access to those groups. This enables the VSA user to view and report on logical collections of related machine IDs, such as laptops, workstations, servers, MS Exchange Servers, etc. Collections are created using the [Only show selected machine IDs](#) checkbox in [View Definitions](#) (page 28). Save a view first before selecting machines IDs using this option. Once the view is saved, a [<N> machines selected](#) link displays to the right of this option. Click this link to display a [Define Collection](#) window, which allows you to create a view using a free-form selection of individual machine IDs.

**Note:** The [Filter Aggregate Table](#) (page 30) provides an alternate method of selecting machine IDs for a view definition, based on standard and user defined attributes.

### Copy Settings and Templates

**Machine ID templates** (page 592) are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > [Copy Settings](#) to copy these changes to any number of machines IDs you are authorized to access. Be sure to select `Do Not Copy` for any settings you do not want to overwrite. Use `Add` to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

### Credential

A credential is the logon name and password used to authenticate a user or process's access to a machine or network or some other resource. See Agent > [Set Credentials](#) (page 83).

## Current VSA Time

The current time used by the KServer is displayed in System > [Preferences](#) (page 391).

## Dashboard

The dashboard is a summary display of the status of the entire system. The dashboard's data is filtered by the [machine ID / group ID filter](#) (page 592). Navigation: Info Center > [View Dashboard](#) (page 180).

## Dashboard List

The dashboard list is a summary display of the alarm statuses of all machines being monitored. The dashboard list's data is filtered by the [machine ID / group ID filter](#) (page 592). Navigation: Info Center > [Dashboard List](#) (page 189) or Monitor > Dashboard List.

## Distribute File

The [Distribute File](#) function sends files stored on your VSA server to managed machines. It is ideal for mass distribution of configuration files, such as virus foot prints, or maintaining the latest version of executables on all machines. The VSA checks the integrity of the file every [full check-in](#) (page 588). If the file is ever deleted, corrupted, or an updated version is available on the VSA, the VSA sends down a new copy prior to any procedure execution. Use it in conjunction with recurring procedures to run batch commands on managed machines.

## Event Logs

An [event log service](#) runs on Windows operating systems (Not available with Win9x). The event log service enables event log messages to be issued by Window based programs and components. These events are stored in event logs located on each machine. The event logs of managed machines can be stored in the KServer database, serve as the basis of alerts and reports, and be archived.

Depending on the operating system, the [event log types](#) available include but are not limited to:

- Application log
- Security log
- System log
- Directory service log
- File Replication service log
- DNS server log

The list of event types available to select can be updated using Monitoring > [Update Lists by Scan](#) (page 203).

Windows events are further classified by the following [event log categories](#):

- Error
- Warning
- Information
- Success Audit
- Failure Audit
- Critical - Applies only to Vista, Windows 7 and Windows Server 2008
- Verbose - Applies only to Vista, Windows 7 and Windows Server 2008

Event logs are used or referenced by the following VSA pages:

- Monitor > [Agent Logs](#) (page 34)
- Monitor > Alerts > [Event Logs](#) (page 234)
- Monitor > Alerts > [Edit Event Sets](#) (page 239)
- Monitor > [Update Lists by Scan](#) (page 203)
- Agent > [Log History](#) (page 35)
- Agent > [Event Log Settings](#) (page 37)
- Agent > [Agent Logs](#) (page 34)

## Glossary of Terms

- Reports > [Logs](#) (page 591)
- System > Database Views > [vNtEventLog](#) (page 497)

## Events Sets

Because the number of events in Windows events logs is enormous the VSA uses a record type called an **event set** to filter an alarm condition.

Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 589) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (\*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

For details on how to configure event sets, see Monitor > Alerts > Event Logs > [Edit Event Sets](#) (page 239).

## File Transfer Protocol (FTP)

**File Transfer Protocol (FTP)** is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. The **FTP server** is the program on the target machine that listens on the network for connection requests from other computers. The **FTP client** is the program on the VSA user's local machine that initiates a connection to the server. The FTP client machine requires user access rights to the FTP server machine. It is included with the KServer primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. Since Kaseya FTP sessions are relayed through the KServer, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

## Flood Detection

If 1000 events—not counting **black list events** (page 590)—are uploaded to the KServer by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your KServer. Alarm detection and processing operates regardless of whether collection is suspended.

## Global Event Log Black Lists

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml`. The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

## Group Alarms

Alert, system check, and log monitoring alarms are automatically assigned to a **group alarm** category. If an alarm is triggered, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the **Group Alarm Status** (page 194) dashlet of the Monitor > [Dashboard List](#) page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > [Monitor Lists](#) (page 202). Group alarm column names are assigned to monitor sets using [Define Monitor Set](#) (page 206).

## Host name

The text equivalent of an IP address. For example, the IP address 89.234.7.197 should resolve to the host name of `www.kaseya.com`.

## Hotfix

Kaseya frequently posts hotfixes to correct small problems in the latest release. If the **Enable automatic check** box is checked in System > [Configure](#) (page 412), your VSA periodically checks for *new only*

hotfixes at <http://vsaupdate.kaseya.net>. If any new hotfixes are available, the KServer automatically downloads and applies the hotfixes without any user interaction.

The hotfix mechanism addresses minor issues only, typically either cosmetic typos, or ASP page errors. The KServer, agents, or database schema are never updated via hotfixes. Any changes affecting system operation go into full product updates that you approve before installing. Hotfixes just correct minor issues without having to wait for the release cycle.

## ISO Image

An **ISO image (.iso)** is a disk image of an ISO 9660 file system. ISO 9660 is an international standard originally devised for storing data on CD-ROM. In addition to the data files that are contained in the ISO image, the ISO image also contains all the filesystem metadata, including *boot code*, structures, and attributes. All of this information is contained in a single file. CD writers typically provide the option of writing an ISO file as *an image* when writing to a CD.

## LAN Watch

LAN Watch uses an existing VSA **agent** (page 583) on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without agents or **SNMP devices** (page 597). Optionally, the VSA can send an **alert** (page 585) when a LAN Watch discovers any new device. LAN Watch effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

## Log Monitoring

The VSA is capable of monitoring data collected from many **standard log files** (page 591). **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and **syslog** (page 599) files created for Unix, Linux, and Macintosh operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the KServer database, **Log Monitoring** uses **parser definitions and parser sets** (page 595) to parse each log file and select only the data you're interested in. Parsed messages are displayed in Log Monitoring, which can be accessed using the Agent Logs tab of **Live Connect** (page 380) > Agent Data or the **Machine Summary** (page 137) page or by generating a report using the Agent > Logs - **Log Monitoring** (page 165) page. Users can optionally trigger alerts when a **Log Monitoring** record is generated, as defined using **Assign Parsing Sets** (page 297) or **Parser Summary** (page 288).

## Logs

Logs collect event information about multiple systems, including the KServer. The different types of logs that can be generated are:

- **Admin Notes** - Lists user notes, sorted by user.
- **Agent Log** - Shows a list of activity associated with the Agent machine Agent. Start and stop times, *.ini* file changes, and other information is captured. The date and time of each activity is also noted.
- **Agent Procedure Log** - Shows a list of procedures executed on the selected agent machine. The date and time of each procedure execution is also noted, as well as whether it completed successfully or not.
- **Alarm Log** - List out all triggered alarms issued against the selected machine.
- **Configuration Changes** - Shows a log of changes made by a user to a managed machine's agent configuration.
- **Event Logs** - Shows the **event log** (page 589) data collected by Windows. (Not available with Win9x)
- **Log Monitoring** - enables you to monitor the data generated by any text-based log.
- **Monitor Action Log** - The log of **alarm conditions** (page 585) that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **Network Statistics** - Shows a list of applications that have accessed the network and the packet size of the information exchanged during the network access session. The time of the exchange is also listed.

## Glossary of Terms

- **Remote Control Log** - Lists successful remote controls sessions.

### MAC address

The unique **media access control (MAC)** identifier assigned to network adapter cards (NICs).

### Machine ID / Group ID / Organization ID

Each **agent** (page 583) installed on a managed machine is assigned a unique **machine ID / group ID / organization ID**. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all the machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.sales.chicago.acme`. In this case `sales` is a subgroup ID within the `chicago` group ID within the organization ID called `acme`. In some places in the VSA, this hierarchy is displayed in reverse order. Each organization ID has a single default machine group ID called `root`. Group IDs and subgroup IDs are created using the System > Orgs/Group/Depts/Staff > Manage > **Machine Groups** (page 410) page.

### Machine ID / Group ID filter

The Machine ID / Machine Group filter is available on all tabs and functions. It allows *you* to limit the machines displayed on *all* function pages. The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. Once filter parameters are specified, click the **Apply** button to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in <All Groups> managed by the currently logged on VSA user.

**Note:** Even if a VSA user selects <All Groups>, only groups the VSA user is granted access to using System > User Security > **Scopes** (page 404) are displayed.

### Machine ID Template

Machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc. **A corresponding install package can be created based on each machine ID template you define.**

- Create machine ID templates using Agent > **Create** (page 49).
- Import a machine ID template using Agent > **Import/Export** (page 71).
- Base an agent install package on a machine ID template using Agent > **Deploy Agents** (page 39).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** (page 70).
- Identify the total number of machine ID template accounts in your VSA using System > **Statistics** (page 423).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Macintosh and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

### Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** (page 592) and the **agent** (page 583). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed

machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

## Machine Roles

The **Machine Roles** (page 400) page creates and deletes machine roles. Machine roles determine what *machine users* see when they use **Portal Access** (page 81)—a version of **Live Connect** (page 380)—from a machine with an agent. The **Portal Access** window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine*.

**Note:** The **User Roles** page determines what *VSA users see when they use Live Connect from within the VSA*.

Within the **Machine Roles** page you can select:

- **Members** (page 403) - Assign or remove machines for a machine role.
- **Access Rights** (page 403) - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- **Role Types** (page 404) - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

## Managed Machine

A monitored machine with an installed **agent** (page 583) and active **machine ID / group ID** (page 592) account on the KServer. Each managed machine uses up one **agent license** (page 420).

## Master User / Standard User

A master user is a VSA **user** (page 600) that uses a **Master** user role and a **Master** scope. The **Master** user role provides user access to all functions throughout the VSA. The **Master** scope provides access to all scope data objects throughout the VSA. A **Master** user role can be used with a non-**Master** scope, but a **Master** scope cannot be used with a non-**Master** role. KServer management configuration and other **specialized functions** (page 400) can only be performed by **Master** role users. **Master** role users have an additional ability to take ownership of user-defined data objects. The term *standard user* is sometimes used to indicate a user that does not use a **Master** user role and a **Master** scope. When VSA users are listed on a page, a background of two alternating shades of *beige* designates **Master** role users. A background of two alternating shades of *grey* designates non-**Master** role users.

## Migrating the KServer

For the latest instructions on migrating an existing KServer to a new machine see Moving the Kserver section in the the KB article latest **Kserver installation and upgrade user guide** ([help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp](http://help.kaseya.com/WebHelp/EN/KServer-Install-Guide.asp)).

## Monitor Sets

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 596), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Update monitor set counter objects, instances and counters by source machine ID using Monitor > **Update Lists by Scan** (page 203).

**Note:** You must run **Update Lists by Scan** (page 203) for each machine ID you assign a monitor set, to ensure a complete list of monitoring definitions exists on the VSA to monitor that machine.

## Glossary of Terms

2. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 202).
3. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 204).
4. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 261).
5. Optionally customize standard monitor sets as *individualized monitor sets*.
6. Optionally customize standard monitor sets using *Auto Learn*.
7. Review monitor set results using:
  - Monitor > **Monitor Log** (page 267)
  - Monitor > **Live Counter** (page 201)
  - Monitor > Dashboard > **Network Status** (page 193)
  - Monitor > Dashboard > **Group Alarm Status** (page 194)
  - Monitor > Dashboard > **Monitoring Set Status** (page 194)
  - Info Center > Reports > Monitor > Monitor Set Report
  - Info Center > Reports > Monitor > Monitor Action Log

### Monitor Types

- 0 - Counter
- 1 - Service
- 2 - Process
- 3 - SNMP
- 4 - Alert - Alerts are further classified using **alert types** (page 586).
- 5 - System Check
- 6 - EPS
- 7 - Log Monitoring

### myOrg

`myOrg` is the **organization** (page 594) of the service provider using the VSA. All other organizations in the VSA are second party organizations doing business with `myOrg`. The default name of `myOrg`, called `My Organization`, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the `myOrg` organization.*

### Org

The VSA supports three different kinds of business relationships:

- **Organizations** - Supports machine groups and manages machines using agents.
- **Customers** - Supports the billing of customers using Kaseya Service Billing.
- **Vendors** - Supports the procurement of materials using Kaseya Service Billing.

The `Org` table is a support table shared by *organizations*, *customers* and *vendors*. Each record in the `Org` table is identified by a unique `orgID`. The `Org` table contains basic information you'd generally need to maintain about any kind of business relationship: mailing address, primary phone number, duns number, yearly revenue, etc. Because the `Org` table is shared, you can easily convert:

- A customer into an organization or vendor.
- A vendor into an organization or customer.
- An organization into a customer or vendor.

**Note:** `myOrg` (page 594) is the organization of the service provider using the VSA.

### Packager

The **Packager** is a wizard tool used to create a package when a pre-defined install solution cannot be

used. **Packager** evaluates the state of a source machine before and after an installation and/or resource change. The **Packager** compiles the differences into a single executable file—the **package**—that can be distributed via agent procedures to any managed machine. Distribute a package any way you choose. You can email it, or store it on a server where a **custom procedure** (page 94) can perform a silent installation on any managed machine.

### Parser Definitions and Parser Sets

When configuring **Log Monitoring** (page 591) it's helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A **parser definition** is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in **Log Monitoring**.

A **parser set** subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts.

Without the filtering performed by the parser set, the KServer database would quickly expand. For example a log file parameter called \$FileServerCapacity\$ might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in **Log Monitoring**, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

### Patch Policy

Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- **Initial Update** (page 313) and **Automatic Update** (page 317) require patches be approved before these patches are installed.
- **Approval by Policy** (page 329) approves or denies patch by *policy*.
- **Approval by Patch** (page 331) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- **KB Override** (page 333) overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- **Patch Update** (page 321) and **Machine Update** (page 319) can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

### Patch Update Order

Service packs and patches are installed in the following order:

## Glossary of Terms

1. Windows Installer
2. OS related service packs
3. OS update rollups
4. OS critical updates
5. OS non-critical updates
6. OS security updates
7. Office service packs
8. Office update rollups
9. All remaining Office updates

**Note:** Reboots are forced after each service pack and at the end of each patch group without warning. This is necessary to permit the re-scan and installation of the subsequent groups of patches.

## Performance Objects, Instances and Counters

When setting up counter thresholds in **monitor sets** (page 593), it's helpful to keep in mind exactly how both Windows and the VSA identify the components you can monitor:

- **Performance Object** - A logical collection of counters that is associated with a resource or service that can be monitored. For example: processors, memory, physical disks, servers each have their own sets of predefined counters.
- **Performance Object Instance** - A term used to distinguish between multiple performance objects of the same type on a computer. For example: multiple processors or multiple physical disks. The VSA lets you skip this field if there is only one instance of an object.
- **Performance Counter** - A data item that is associated with a performance object, and if necessary, the instance. Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance.

## Portal Access

Portal Access is a **Live Connect** (page 380) session initiated by the machine user. The machine user displays the **Portal Access** page by clicking the agent icon  on the system tray of a managed machine. **Portal Access** contains machine user options such as changing the user's contact information, creating or tracking trouble tickets, chatting with VSA users or remote controlling their own machine from another machine. **Portal Access** logons are defined using Agent > **Portal Access** (page 81). The function list the user sees during a **Portal Access** session is determined by the System > **Machine Roles** (page 403) page. You can customize **Portal Access** sessions using the System > Customize > **Live Connect** (page 432) page.

## Primary Domain Controller

Primary domain controllers have full access to the accounts databases stored on their machines. Only primary domain controllers run **Active Directory** (page 583).

## Private Folders

### Private Folders

Objects you create—such as reports, procedures, or monitor sets—are initially saved in a folder with your user name underneath a **Private** cabinet. This means only you, the creator of the objects in that folder, can view those objects, edit them, run them, delete them or rename them.

To share a private object with others you first have to drag and drop it into a folder underneath the **Shared** cabinet.

**Note:** A master role user can check the **Show shared and private folder contents from all users** checkbox in **System > Preferences** (page 391) to see all shared and private folders. For Private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

## Quick Status

A **Quick Status** feature enables you to select *any* monitor set counter, service or process from *any* machine ID and add it to the same single display window. Using **Quick Status**, you can quickly compare the performance of the same counter, service or process on different machines, or display selected counters, services and processes from different monitor sets all within a single view. SNMP sets provide a similar **Quick Status** view for selected SNMP objects. *Any Quick Status view you create exists only for the current session.* The **Quick Status** window is accessed using Monitor > Dashboard > **Monitoring Set Status** (page 194), then clicking the **Quick Status** link or the **Quick Status** icon .

## Silent Install

Silent installs, also called **silent deploys**, do not prompt the user for input. Silent installs may not require user input or else provide a typical configuration that serves the purposes of most users, or else provide command line parameters that enable users to configure the installation at execution. If an install does not support a silent install but still needs to be distributed automatically, users can use **Packager** (page 594) to create a custom installation package. See **Creating Silent Installs** (page 125).

## SNMP Community

An SNMP community is a grouping of devices and management stations running SNMP. SNMP information is broadcast to all members of the same community on a network. SNMP default communities are:

- Write = private
- Read = public

## SNMP Devices

Certain network devices such as printers, routers, firewalls, servers and UPS devices can't support the installation of an **agent** (page 583). But a VSA agent installed on a managed machine on the same network as the device can read or write to that device using **simple network management protocol (SNMP)**.

## SNMP Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **LAN Watch** (page 272) is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > **SNMP Sets** and in the drop-down list in Monitor > **Assign SNMP**. A (QS) prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 272).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 276).
3. Click the hyperlink underneath the name of the device, called the **SNMP info** (page 281) link, in the **Assign SNMP** page to display a dialog.
  - Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
  - Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.
  - Enter a name after the (QS) prefix in the header of the dialog.
  - Click the **Apply** button to apply the quickset to the device.

4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** (page 284), the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > **SNMP Sets** (page 598).

### SNMP Sets

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 597). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 597) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 598) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 272).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 276). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 284) or **Dashboard List** (page 189).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 202).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 212).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 217).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 287).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 286).

### SNMP Types

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value 77 for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a LAN Watch.

**Note:** The entire OID for `system.sysServices.0` is `.1.3.6.1.2.1.1.7.0` or `.iso.org.dod.internet.mgmt.mib-2.system.sysServices.`

You can assign **SNMP sets** (page 598) to **devices** (page 597) *by type automatically* as follows:

1. Add or edit SNMP *types* using the **SNMP Device** tab in Monitor > **Monitor Lists** (page 202).
2. Add or edit the value returned by the MIB object `system.sysServices.0` *and associated with each SNMP type* using the **SNMP Services** tab in Monitor > **Monitor Lists**.
3. Associate a SNMP *type* with a SNMP *set* using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > **Define SNMP Set** (page 213).

4. Perform a **LAN Watch** (page 272). During the LAN Watch SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a value for the `system.sysServices.0` MIB object that matches the SNMP type associated with those SNMP sets.

You can also assign **SNMP sets** (page 598) to **devices** (page 597) *manually* as follows:

- Assign a SNMP type to an SNMP device using Monitor > **Set SNMP Type** (page 287). Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

### Software as a Service (SaaS)

Kaseya provides "software as a service" (SaaS) deployment of **Virtual System Administrator™**. Service providers contract with Kaseya to access a VSA hosted and maintained by Kaseya and can install a specified number of their customer agents. Service providers only see their own organizations, machine groups, procedures, reports and tickets on the SaaS VSA. Service providers have full access to all the functions of the VSA except system maintenance, which is the responsibility of Kaseya.

### syslog

Syslog is a standard for forwarding log messages in an IP network to a syslog server. A syslog server collects the messages broadcast by various devices on the network and integrates them into a centralized repository of syslog files. Syslog is commonly used by Unix, Linux and Macintosh operating systems and hardware devices such as Cisco routers. **Log Monitoring** (page 591) enables you to monitor syslog files.

A typical format for a syslog file entry is:

```
<time> <hostname> <tag>:<message>
```

For example:

```
Oct 15 19:11:12 Georges-Dev-Computer kernel[0]: vmnet: bridge-en1: interface
en is going DOWN
```

### System Agent Procedures

System agent procedures are basic functions that are exposed by the VSA. You can schedule system agent procedures to run automatically. They cannot be edited nor can they accept parameters. A list of available system agent procedures displays in any Agent Procedure Search popup window. System agent procedures can be run from:

- Within a parent procedure using the **Execute Procedure** or **Schedule Procedure** commands of an **IF-ELSE-STEP** (page 97) statement.
- Any alerts page using the **Run Agent Procedure** checkbox.
- The **Pending Procedures** tab in **Live Connect** (page 380) or the **Machine Summary** (page 137) page.

Because a system agent procedure can be run using an alert or parent agent procedure associated with a specific machine ID account, the scheduling of a system agent procedure can be copied, typically from a machine ID template to a machine using Agent > **Copy Settings** (page 70).

### System Checks

The VSA can monitor machines that *don't have an agent installed on them*. This function is performed entirely within a single page called **System Check**. Machines without an agent are called **external systems**. A machine with an agent is assigned the task of performing the system check on the external system. A system check typically determines whether an external system is available or not. Types of system checks include: web server, DNS server, port connection, ping, and custom.

### System Tray

The system tray is located, by default, in the lower right-hand corner of the Windows desktop, in the Taskbar. It contains the system clock, and other system icons.

## Glossary of Terms

### User Account

See [Machine IDs vs. Agents](#) (page 592)

### Users

VSA users use the VSA application to maintain the KServer and oversee the monitoring of [managed machines](#) (page 593) by the KServer and its [agents](#) (page 583). VSA users are created using System > [Users](#) (page 397). Users also refers to machine users, who use the computers managed by the VSA. [Master users](#) (page 593) have special privileges throughout the VSA.

### View Definitions

The [View Definitions](#) (page 28) window lets you further refine a machine ID / group ID filter based on attributes contained on each machine—for example, the operating system type. Views provide users flexibility for machine management and reporting. View filtering is applied to *all* function pages by selecting a view from the [Select View](#) drop-down list on the [machine ID / group filter](#) (page 26) panel and clicking the Apply icon . Any number of views can be created and shared with other users. Views are created by clicking the [Edit](#) button to the right of the [Views](#) drop-down list.

### Virtual Machine

A virtual machine (VM) is a software implementation of a physical computer (machine) that executes programs like a physical computer. Virtual machines are capable of virtualizing a full set of hardware resources, including a processor (or processors), memory and storage resources and peripheral devices. The [Backup](#) module can convert a backup image into a VM. See Backup > Image to VM.

### Virtual Network Computing (VNC)

[Virtual Network Computing \(VNC\)](#), also called [remote control](#) or [remote desktop](#), is a graphical desktop sharing system which uses the Remote Framebuffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. It is included with the KServer primarily to provide immediate technical support. VNC is platform-independent. A VNC viewer on any operating system can usually connect to a VNC server on any other operating system. The [VNC server](#) is the program on the remote machine that shares its screen. The [VNC client \(or viewer\)](#) is the program on the local machine that watches and interacts with the remote machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the KServer, all VNC sessions are protected by the Kaseya 256 bit rolling encryption protocol.

### vPro

Intel® vPro™ Technology provides hardware-based management integration independent of operating system software and network management software. The VSA can discover vPro-enabled machines during a [LAN Watch](#) (page 591), list the hardware assets of vPro machines, access hardware-based security use the power management and remote booting of ISO images capabilities provided by vPro.

### Windows Automatic Update

Windows Automatic Updates is a Microsoft tool that automatically delivers updates to a computer. Windows Automatic Updates is supported in the following operating systems: Windows 2003, Windows XP, Windows 2000 SP3 or later, and all operating systems released after these. Patch Management > [Windows Auto Update](#) (page 335) can enable or disable this feature on managed machines. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems can.

### Work Types

Work types determine how time entries are integrated with other functions in the VSA. The work type options displayed in your VSA depend on the modules installed.

- [Admin Tasks](#) - A recurring operational activity not associated with any project.
- [Work Orders](#) - Only displays if the [Kaseya Billing Service](#) is installed.

- **Service Desk Tickets** - Only displays if **Kaseya Service Desk 1.3** or later is installed.



# Index

## 6

64-Bit Commands • 114

## A

Access Policy • 445  
 Active Directory • 583  
 Add SNMP Object • 217  
 Add/Remove • 142  
 AddIncident • 566  
 AddIncident Request • 579  
 AddIncident Response • 579  
 AddMachGroupToScope • 522  
 AddOrg • 523  
 AddOrgDeptStaff • 523  
 AddOrgToScope • 523  
 AddScope • 523  
 AddScopeOrg • 524  
 AddScriptAssignment • 553  
 AddScriptPrompt • 553  
 AddServDeskToScope • 566  
 AddTicRequest • 524  
 AddUserToRole • 524  
 AddUserToScope • 524  
 AdminGroupAccess • 525  
 Administrative Tasks • 467  
 Administrator Notes • 14  
 Advanced Filtering • 30  
 Agent • 21  
 Agent Icons • 25  
 Agent Install Command Line Switches • 44  
 Agent Logs • 34  
 Agent Menu • 73, 583  
 Agent Overview • 23  
 Agent Procedure API Web Service • 552  
 Agent Procedure API Web Service - Operations • 552  
 Agent Procedure Editor • 96  
 Agent Procedure Status • 122  
 Agent Procedures • 91  
 Agent Procedures Overview • 93  
 Agent Quick View Window • 583  
 Agent Settings • 583  
 Agent Status • 31  
 Agents • 16, 24, 584  
 Agents - Linux • 584  
 Agents - Macintosh • 584  
 Alarm • 585  
 Alarm Condition • 585  
 Alarm List • 191  
 Alarm Network Status • 191  
 Alarm Rotator • 193  
 Alarm Summary • 198  
 Alarm Summary Window • 192  
 Alarm Ticker • 193

Alarms • 187  
 Alarms - Suspending • 585  
 Alert • 585  
 Alert Types • 586  
 Alerts • 219  
 Alerts - Agent Procedure Failure • 243  
 Alerts - Agent Status • 222  
 Alerts - Application Changes • 225  
 Alerts - Backup Alert • 252  
 Alerts - Event Logs • 234  
 Alerts - Get Files • 227  
 Alerts - Hardware Changes • 229  
 Alerts - LAN Watch • 240  
 Alerts - Low Disk • 232  
 Alerts - New Agent Installed • 247  
 Alerts - Patch Alert • 249  
 Alerts - Protection Violation • 245  
 Alerts - Summary • 220  
 Alerts - System • 256  
 Anti-Malware - Anti-Malware Installation Statistics • 153  
 Antivirus - Antivirus Installation Statistics • 152  
 API • 513  
 API Web Services • 511  
 Application Blocker • 89  
 Application Deploy • 124  
 Application Logging • 460  
 Application Logging • 426  
 Approval by Patch • 331  
 Approval by Policy • 329  
 Approval Patterns • 467  
 Approve Timesheets • 459  
 Assign Monitoring • 261  
 Assign Parser Sets • 297  
 Assign SNMP • 276  
 Assignee Policy • 446  
 AssignEventAlertToMachine • 554  
 AssignEventLogMachineSettings • 554  
 AssignRole • 525  
 AssignScope • 525  
 ATSE Response Code • 587  
 Attachment • 560  
 Audit • 131, 587  
 Audit - Aggregate Table • 153  
 Audit - Disk Utilization • 153  
 Audit - Inventory • 153  
 Audit - Machine Changes • 154  
 Audit - Machine Summary • 154  
 Audit - Network Statistics • 155  
 Audit Overview • 133  
 Audit Summary • 135  
 Authenticate • 525  
 AuthenticateWithAppSessionID • 526  
 Auto Learn - Monitor Sets • 266  
 Auto Learn - SNMP Sets • 283  
 Auto Learn Monitor Sets • 587  
 Automatic Update • 317

## B

Backup > Backup • 156  
 Backup Sets • 587  
 Bookmarks • 15

## Index

### C

- Cancel Script • 137
- Cancel Updates • 325
- Canonical Name • 587
- Change Group • 56
- Change Logon • 392
- Chat • 373, 587
- Check-in
  - Full vs. Quick • 588
- Check-In Control • 75
- Check-in Icons • 16
- Check-in Policy • 393
- Check-in Status • 588
- CloseAlarm • 526
- Collection • 588
- Color Scheme • 16, 428
- Command Line • 348
- Configuration • 1
- Configure • 412
- Configure Column Sets • 137
- Configuring Patch Management • 306
- Configuring the Server • 3
- Configuring Time Tracking • 455
- Control Machine • 356
- Copy Settings • 70
- Copy Settings and Templates • 588
- Counter Thresholds • 208
- Create • 49
- Create a New Master User • 400
- Create/Delete
  - Patch Policy • 326
- Create/View • 438
- CreateAdmin • 526
- CreateAgentInstallPackage • 527
- CreateEventSet • 555
- CreateEventSetDefinition • 555
- CreateMachineGroup • 527
- CreateRole • 527
- Creating a Customer / Work Order Timer Entry • 463
- Creating a Customer / Work Order Timesheet Entry • 458
- Creating a Service Desk Ticket and Service Billing Timer Entry • 464
- Creating a Service Desk Ticket or Ticket/Task Timer Entry • 465
- Creating a Service Desk Ticket Timesheet Entry • 458
- Creating an Administrator Task Timer Entry • 463
- Creating an Administrator Task Timesheet Entry • 458
- Creating Custom Agent Icons • 430
- Creating Organizations Automatically During Update • 6
- Creating Silent Installs • 125
- Credential • 588
- Crystal Reporting Usage • 473
- Current VSA Time • 589
- CustomField • 560
- Customize
  - Live Connect • 432
- Customize • 180, 428
- Customized New Ticket Link • 383

### D

- Dashboard • 589
- Dashboard List • 189, 589
- Dashboard Settings • 197
- Data Table Column Options • 18
- Database Views • 469, 472
- Define Monitor Sets • 206
- Define SNMP Set • 213
- Delete • 53
- Delete/Archive • 441
- DeleteAdmin • 527
- DeleteAgent • 527
- DeleteAgentInstallPackage • 528
- DeleteAllEventAlertsFromMachine • 555
- DeleteAllEventLogMachineSettings • 555
- DeleteEventAlertFromMachine • 556
- DeleteEventLogMachineSettings • 556
- DeleteEventSet • 556
- DeleteEventSetDefinition • 556
- DeleteMachineGroup • 528
- DeleteOrg • 528
- DeleteRole • 528
- DeleteScope • 529
- Deploy Agents • 39
- Desktop Policy - Desktop Policy • 156
- Desktop Policy - Power Savings • 156
- Device Status • 196
- DisableAdmin • 529
- Distribute File • 129, 589
- Distribution • 120
- Documents • 143
- Domain Logon • 66, 391
- Due Date Policy • 447

### E

- Echo • 529, 553
- EchoMt • 529, 553
- Edit Event Sets • 239
- Edit Fields • 448
- Edit Profile • 79
- Email Mapping • 451
- Email Reader • 449
- Embedding the VSA Logon Form in Web Pages • 388
- EnableAdmin • 529
- Enabling KSD API Web Service • 559
- Enabling the Agent Procedure API Web Service • 552
- Enabling the Monitoring API Web Service • 554
- Enabling Ticketing for Portal Access Users on Unsupported Browsers • 82
- Enabling VSA API Web Service • 514
- Event Log Settings • 37
- Event Logs • 589
- Events Sets • 590
- Excel Usage • 472
- Executive - Executive Summary • 158

### F

- File Access • 85
- File Source • 340
- File Transfer Protocol (FTP) • 590

Filter Aggregate Table • 30  
 Flood Detection • 590  
 fnMissingPatchCounts\_UsePolicy /  
   fnMissingPatchCounts\_NoPolicy • 478  
 fnOSCounts • 479  
 Folder Rights • 119  
 FTP • 370

## G

Get File • 127  
 GetAlarm • 530  
 GetAlarmList • 531  
 GetEventAlertList • 556  
 GetEventLogMachineSettingsList • 557  
 GetEventSetDefinitionList • 558  
 GetEventSetList • 558  
 GetGroupLicenseInfo • 531  
 GetIncident • 566  
 GetIncident Request • 577  
 GetIncident Response • 577  
 GetIncidentList • 567  
 GetIncidentList Request • 577  
 GetIncidentList Response • 577  
 GetLogEntry • 532  
 GetMachine • 532  
 GetMachineCollectionList • 535  
 GetMachineGroupList • 535  
 GetMachineList • 535  
 GetMachineUptime • 536  
 GetNotesList • 536  
 GetOrgLocation • 537  
 GetOrgs • 537  
 GetOrgsByScopeID • 537  
 GetOrgTypes • 538  
 GetPackageURLs • 538  
 GetPartnerUserLocation • 538  
 GetPublishedViewColumns • 539  
 GetPublishedViewRows • 540  
 GetPublishedViews • 541  
 GetRoles • 544  
 GetScopes • 544  
 GetScriptAssignmentId • 553  
 GetScriptIdFromScriptName • 554  
 GetServiceDesk • 568  
 GetServiceDesk Request • 570  
 GetServiceDesk Response • 570  
 GetServiceDesks • 568  
 GetServiceDesks Request • 569  
 GetServiceDesks Response • 569  
 GetSessionDetails • 544  
 GetTicket • 545  
 GetTicketList • 546  
 GetTicketNotes • 546  
 GetTicRequestTicket • 547  
 Getting Started • 9  
 GetVerboseMachineGroupList • 547  
 Global Event Log Black Lists • 590  
 Group Alarm Status • 194  
 Group Alarms • 590

## H

Host name • 590  
 Hotfix • 590

## I

If Your Account Is Disabled • 400  
 IF-ELSE-STEP Commands • 97  
 Import / Export • 71  
 Import Center • 422  
 Inbox • 147  
 Incident • 564  
 Incident Summary • 563  
 Info Center • 145  
 Initial Update • 313  
 Install Agents • 60  
 Install Issues and Failures • 45  
 Installed Applications • 141  
 Installing Linux Agents • 47  
 Installing Multiple Agents • 45  
 ISO Image • 591

## K

KB Override • 333  
 KES Status • 197  
 KES Threats • 197  
 KSD API Web Service • 559  
 KSD API Web Service - Operations • 566  
 KSD API Web Service Data Types • 559

## L

LAN Watch • 56, 272, 591  
 Layout Dashboard • 181  
 Learning More • 19  
 License Manager • 420  
 Live Connect • 17  
 Live Connect • 380  
 Live Counter • 201  
 Local Settings • 431  
 LockFunctionAccess • 547  
 Log File Parser Definition • 293  
 Log File Set Definition • 301  
 Log History • 35  
 Log Monitoring • 591  
 Log Parser • 292  
 Logoff • 15  
 Logon and Browser Settings • 4  
 Logon Hours • 407  
 Logon Policy • 425  
 Logs • 591  
 Logs - Admin Notes • 163  
 Logs - Agent Log • 163  
 Logs - Agent Procedure • 163  
 Logs - Alarm Log • 163  
 Logs - Configuration Changes • 164  
 Logs - Event Logs • 164  
 Logs - Event Logs Frequency • 164  
 Logs - KES Log • 165  
 Logs - Log Monitoring • 165  
 Logs - Logs • 162  
 Logs - Network Statistics Log • 166

## Index

Logs - Remote Control • 166

## M

MAC address • 592  
Machine History • 318  
Machine ID / Group ID / Organization ID • 592  
Machine ID / Group ID filter • 592  
Machine ID / Machine Group Filter • 26  
Machine ID Template • 592  
Machine IDs vs. Agents • 592  
Machine Policy • 368  
Machine Roles • 593  
Machine Roles • 403  
Machine Status • 196  
Machine Summary • 137  
Machine Update • 319  
Machines Online • 196  
Macintosh • 39, 56, 60, 78, 430, 584  
Manage • 408  
Manage Files Stored on Server • 118  
Managed Machine • 593  
Master User / Standard User • 593  
Master User vs. Standard Users • 399  
Membership  
    Patch Policy • 327  
Methods of Updating Patches • 306  
Migrate • 3, 71, 75, 412, 593  
Migrate Tickets • 443  
Migrating the KServer • 593  
Minimum System Requirements • 3  
Monitor • 183  
Monitor Icons • 211  
Monitor Lists • 202  
Monitor Log • 267  
Monitor Overview • 185  
Monitor Sets • 204, 593  
Monitor Status • 196  
Monitor Types • 594  
Monitoring - Monitor 95th Percentile • 166  
Monitoring - Monitor Action Log • 167  
Monitoring - Monitor Alarm Summary • 167  
Monitoring - Monitor Configuration • 168  
Monitoring - Monitor Log • 168  
Monitoring - Monitor Set • 168  
Monitoring - Monitor Trending • 168  
Monitoring - Uptime History • 169  
Monitoring API Web Service • 554  
Monitoring API Web Service - Operations • 554  
Monitoring Set Status • 194  
My Timesheets • 457  
myOrg • 594

## N

Naming Policy • 395  
Network Access • 87  
Network Health Score • 159  
Network Status • 193  
Note • 560  
Notify Policy • 443

## O

Office Source • 346  
Org • 594  
Orgs/Groups/Depts/Staff • 408  
Outbound Email • 426

## P

Packager • 127, 594  
Page Layout • 11  
Parser Definitions and Parser Sets • 595  
Parser Summary • 288  
Patch - Patch Management • 169  
Patch Alert • 342  
Patch Deploy • 123  
Patch Failure • 308  
Patch Location • 351  
Patch Management • 303  
Patch Management Overview • 305  
Patch Policy • 595  
Patch Processing • 307  
Patch Status • 312  
Patch Update • 321  
Patch Update Order • 595  
Performance Objects, Instances and Counters • 596  
Periods • 466  
Portal Access • 81, 596  
Power Management • 377  
Pre/Post Procedure  
    Patch Management • 315  
Preferences • 391  
Preinstall RC • 364  
Primary Domain Controller • 596  
Primitives • 547, 569  
Private Folders • 596  
Process Status • 210  
Processing Hotfixes Manually • 417  
Publishing a Report Immediately • 151

## Q

Quick Status • 597

## R

Reboot Action • 337  
Refltem • 559  
RelatedIncident • 560  
Remote Control • 353  
Remote Control Overview • 355  
Remote ISO Boot • 378  
RemoveUserFromRole • 549  
Rename • 54  
Report Definitions • 149  
Report Folder Trees • 150  
Report Set Definitions • 178  
Report Set Folder Trees • 178  
Reports • 149  
Reports Sets • 177  
Request Support • 412  
Reset Password • 360  
ResetPassword • 549  
RoleMembership • 549

Rollback • 324  
Run Audit • 134

## S

Sample Messages • 569  
Scan Machine • 310  
Schedule • 147  
Schedule / Create • 94  
Scheduling a Report • 151  
Scheduling a Report Set • 179  
Scopes • 404  
Script, Cancel • 137  
Security - Security • 170  
Select Type • 362  
Send Message • 375  
SendAdminMessage • 549  
Server Management • 412  
Service Desk - Custom Tickets • 170  
Service Desk - Service Goals • 171  
Service Desk - Service Hours • 172  
Service Desk - Service Times • 172  
Service Desk - Service Volumes • 172  
Service Desk - Tickets • 173  
ServiceDeskDefinition • 561  
Services Check • 210  
Set Credential • 83  
Set Parameters • 363  
Set SNMP Type • 287  
Set SNMP Values • 286  
Set URL to MS-SQL Reporting Services Engine • 418  
SetAdminPassword • 550  
SetGroupLicenseInfo • 550  
SetPartnerUserLocation • 550  
Settings • 466  
Set-up Types • 411  
Sharing User-Owned Objects • 406  
Silent Install • 597  
Site Customization • 428  
SNMP Community • 597  
SNMP Devices • 597  
SNMP Icons • 218  
SNMP Log • 284  
SNMP Quick Sets • 281, 597  
SNMP Set Details • 215  
SNMP Sets • 212, 598  
SNMP Traps Alert • 257  
SNMP Types • 598  
Software - Software Applications Changed • 173  
Software - Software Applications Installed • 174  
Software - Software Licenses • 174  
Software - Software Licenses Summary • 174  
Software - Software Operating Systems • 175  
Software as a Service (SaaS) • 599  
Software Licenses • 143  
Special Fields • 514  
Statistics • 423  
Status Monitor • 13  
Superseded Patches • 307  
Supported Linux Functions • 48  
Supported Macintosh Functions • 49  
Suspend • 72  
Suspend Alarms • 199

syslog • 599  
System • 385  
System Activity • 159  
System Agent Procedures • 599  
System Check • 269  
System Checks • 599  
System Info • 140  
System Log • 423  
System Overview • 387  
System Preferences • 393  
System Security • 3  
System Tray • 599

## T

Task Manager • 372  
Ticketing • 433  
Ticketing - Customizable Ticketing • 175  
Ticketing - Ticketing • 176  
Ticketing Overview • 435  
Time Tracking • 453  
Time Tracking - Timesheet Entries • 177  
Time Tracking - Timesheet Summary • 177  
Time Tracking Overview • 455  
Timers • 461  
Timesheet History (Details) • 461  
Timesheet History (Summary) • 461  
Timesheet Summary • 460  
Toolbox • 13  
Top N - Monitor Alarm Chart • 197

## U

Uninstall RC • 366  
Update Agent • 84  
Update Classification • 308  
Update Lists By Scan • 203  
UpdateIncident • 569  
UpdateIncident Request • 579  
UpdateIncident Response • 581  
UpdateOrg • 550  
UpdateTicket • 550  
UpdateUser • 552  
Updating or Moving the VSA • 3  
User Account • 600  
User History • 408  
User Role Policy • 367  
User Roles • 400  
User Security • 397  
User Settings • 391  
Users • 600  
Users • 397  
Using Variables • 115

## V

vAddRemoveList • 480  
vAdminNotesLog • 480  
vAgentConfiguration • 480  
vAgentLabel • 482  
vAlertLog • 482  
Variable Manager • 117  
vBackupLog • 483  
vBaseApplicationInfo / vCurrApplicationInfo • 484

## Index

vBaseCpuInfo / vCurrCpuInfo • 485  
vBaseDiskInfo / vCurrDiskInfo • 485  
vBaseDriveManufacturer / vCurrDriveManufacturer • 486  
vBasePciInfo / vCurrPciInfo • 486  
vBasePrinterInfo / vCurrPrinterInfo • 487  
vCollectionMember • 487  
vConfigLog • 488  
Video Streaming • 359  
View AD Computers • 65  
View AD Users • 66  
View Dashboard • 180  
View Definitions • 28, 600  
View LAN • 64  
View Summary • 435  
View vPro • 69  
Viewing Log Monitoring Entries • 302  
Viewing Published Reports and Reports Set • 152  
Views Provided • 477  
Virtual Machine • 600  
Virtual Network Computing (VNC) • 600  
vkadComputers • 488  
vkadUsers • 489  
vLicenseInfo • 489  
vMachine • 490  
vMonitorAlarmAlert • 492  
vMonitorAlarmCounter • 493  
vMonitorAlarmProcess • 494  
vMonitorAlarmService • 494  
vMonitorAlarmSNMP • 495  
vMonitorAlarmSystemCheck • 496  
vNetStatsLog • 497  
vNtEventLog • 497  
vOnBoardDeviceInfo • 498  
vPatchApprovalStatus • 498  
vPatchConfiguration • 499  
vPatchPolicy • 501  
vPatchPolicyMember • 502  
vPatchStatus • 502  
vPortInfo • 504  
vPro • 600  
VSA API Web Service • 513  
VSA API Web Service - Operations • 522  
VSA API Web Service - Overview • 513  
VSA API Web Service Sample Client - ASP Page • 516  
VSA API Web Service Sample Client - C# GUI application • 515  
VSA API Web Service Security • 519  
VSA Logon Policies • 388  
VSA Modules • 11  
vScriptLog • 505  
vScriptStatus • 505  
vSystemInfo • 506  
vSystemInfoManual • 507  
vTicketField • 507  
vTicketNote • 508  
vTicketSummary • 508  
vUptimeHistory • 509  
vvProAssetDetails • 509

Windows Auto Update • 335  
Windows Automatic Update • 600  
Work Types • 600  
Working Directory • 78

## W

Web Links - Inbound and Outbound • 521