Kaseya 2

Agent Configuration and Deployment

Quick Start Guide

for VSA 6.1

May 16, 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

Understanding Agents

One of the unique features of the VSA is the ability to work with multiple machines or individual machines—across domains, clients, locations or any structure defined. This greatly increases the ability to create and use “best practices”, increases flexibility and greatly decreases the amount of time it takes to complete tasks. Your understanding of the following agent deployment foundation concepts will greatly streamline your successful management of machines using the VSA.

Details for the topics discussed in this document can be found in the online user assistance system. User assistance is context sensitive. Please refer to it from within the VSA application.

Review the following agent deployment foundation concepts before configuring agents for the first time.

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 can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA machine ID / group ID / organization ID. 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 inside the VSA.
- Multiple agents can be installed on the same machine, each pointing to a different server.
- A check-in icon 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. **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** immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

Machine IDs vs Agents

When discussing agents it is helpful to distinguish between the machine ID / group ID / organization ID and the agent. 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.

> **Note:** Machine ID templates are discussed in **Configuring Agent Settings** *(page 7)*.

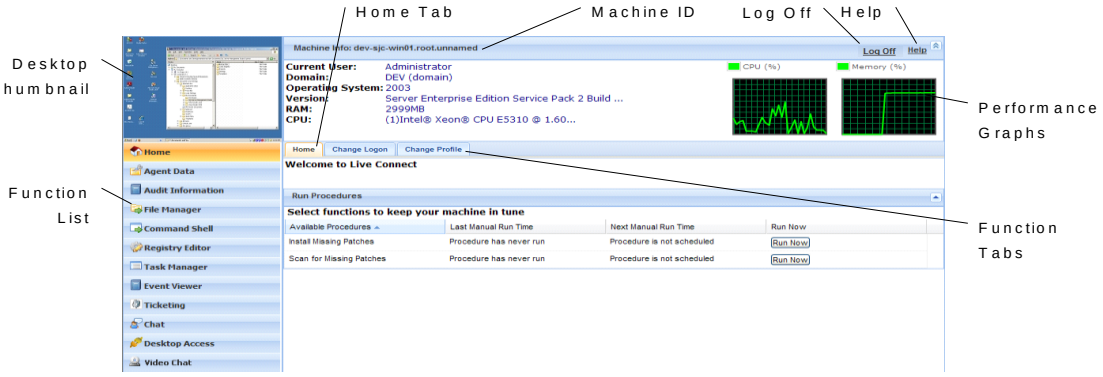
Agent Status Icons in the VSA

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. Hovering the cursor over a check-in icon displays the agent quick view window.

- 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.*
- **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.

The Machine ID / Group ID / Organization ID Hierarchy

Each agent 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.

Example 1: Parent Organizations and Child Organizations

A organization can be the child of another organization.

Parent Organization

- Corporate HQ
  - Department 1, 2, 3, ...

Child Organization

- Company A
  - Department 1, 2, 3, ...
- Company B
  - Department 1, 2, 3, ...
- Company C
  - Department 1, 2, 3, ...

Example 2: Group and Sub-Group

Machine groups are members of organizations. Machine sub-groups are members of machine groups.

Groups:

- Sales
- Marketing
- Accounting
- Production
- IT
- Administration

Sub-Groups:

- Servers
- Desktops
- Notebooks
- Power Users
- Standard Users
- Mobile Users

Example 3: Group and Sub-Group

Groups:

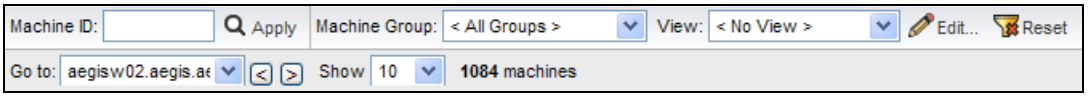
- Client 1
- Client 2
- Client 3
- Client 4

Sub-Groups:

- Sales
- Marketing
- Administration
- Accounting

Filtering Machine ID Accounts

Scopes in System > User Security restricts the machine ID accounts you're allowed to see. In contrast, the **Machine ID / Machine Group** filter allows *you* to decide how to further limit the display of machines you have access to. The Machine ID / Machine Group filter is displayed at the top of *all* function pages that display machine ID accounts.

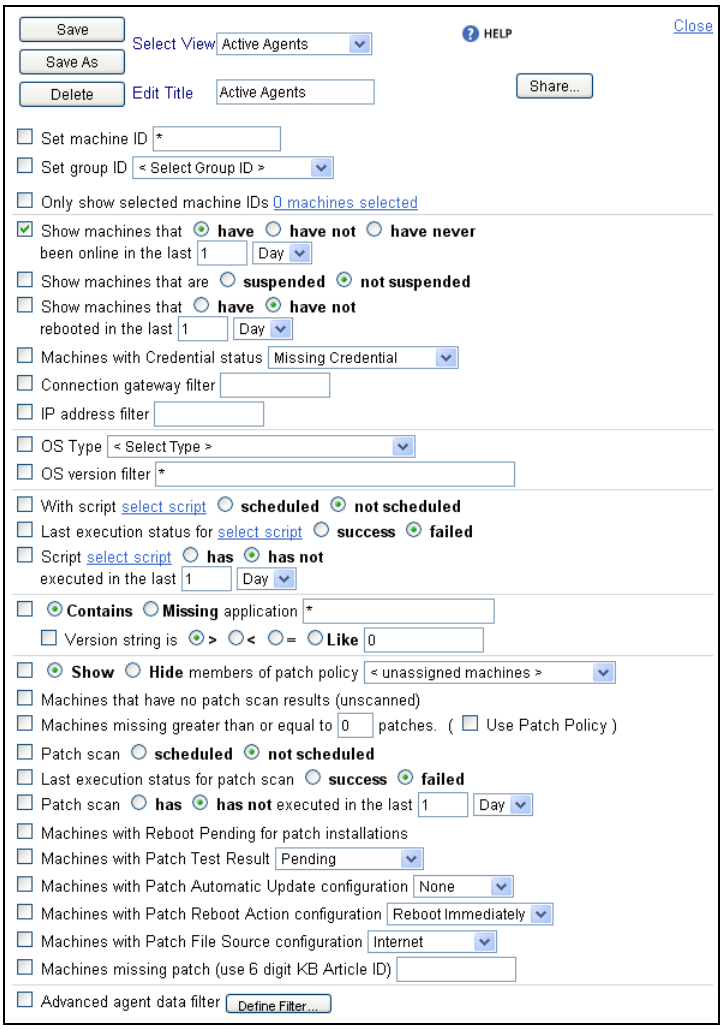


Once filter parameters are specified, click the Apply icon to apply filter settings to *all* function pages. By default, the Machine ID / Machine Group filter displays all machine IDs in `<All Groups>` managed by the currently logged in user.

> **Note:** Even if a user selects `<All Groups>`, only groups the user is granted access to using System > Scopes are displayed.

View Definitions

The View Definitions 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 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.



Creating Views of Selected Machine IDs

You can select a free-form set of *individual machine IDs within a view*. It doesn't matter which groups the machine IDs belong to, so long as the user is authorized to have access to those groups. This enables the user to view and report on logical sets of related machine IDs, such as laptops, workstations, servers, MS Exchange Servers, etc. Machines are selected within a view using the **Only show selected machine IDs** checkbox in **View Definitions**. 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 window which allows you to create a view using a free-form selection of individual machine IDs.

Agents on Managed Machines

Agent Icons on Managed Machines

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.

Note: You can fully customize agents icon using System > Site Customization. See Creating Custom Agent Icons. 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**.

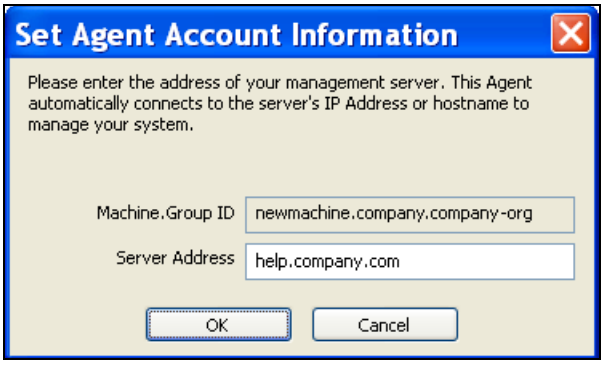
Note: Double clicking the agent icon displays the Portal Access Welcome Page.

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 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.



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.

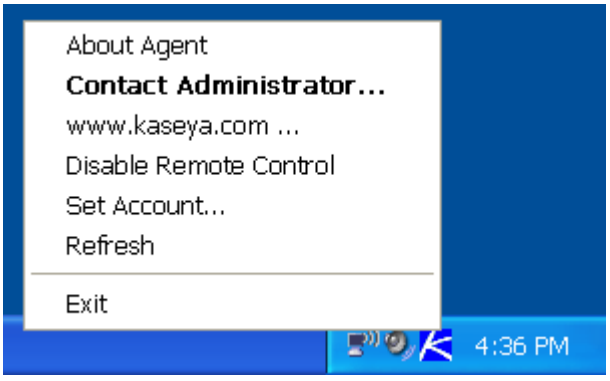
Agent Icon Background Flashes between White and Blue

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 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 for a description of how to turn these options on or off.

Disabling the Agent Menu

VSA users may completely disable the agent menu and remove the icon from the machine's desktop.

Configuring Agent Settings

Agent Settings

Before you install agents to managed machines, you need to decide on the agent settings to use. Agent settings determine the behavior of of the agent on the managed machine. Although each agent can be configured individually, it's easier to managed machines if you adopt similar settings for each type of machine you manage. For example, laptops, desktops and servers could all have settings that

are unique to that type of machine. Similarly, machines for one customer may have unique characteristics that differ from the machines used by other customers.

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
- Agent Menu
- Check-in Control
- Working Directory
- Logs
- Machine Profile - Refers to settings in Audit > Edit Profile.
- 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 except for Event Log alerts and System alerts.
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Agent Procedure Schedules

Once these settings are configured the way you want them for a single managed machine, you can create a new install package. The new package will install the same set of agent settings on any managed machine.

Machine ID Templates

Using *all* the agent settings appropriate for a working machine poses some drawbacks. For example, the credential and patch file source for a working machine *will not work* on a newly managed machine if that machine belongs to another organization.

The solution is to use **machine ID templates** to configure agent settings. 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.
- Import a machine ID template using Agent > Import/Export.
- Base an agent install package on a machine ID template using Agent > Deploy Agents.
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > Copy Settings.
- Identify the total number of machine ID template accounts in your VSA using System > Statistics.
- 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.

To apply a machine ID template to a package:

1. Use the **Create Package** wizard in **Deploy Agent** to use the template as the source machine ID to copy settings from when creating the package to install.
2. Add additional attributes to the package using this same wizard. These additional attributes usually differ from one customer to the next and therefore cannot be usefully stored in the template.

Copying Agent Settings

Machine ID templates 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.

Templates and Filtered Views

There is a corresponding relationship between machine ID templates and filtering your view of selected machines using the **Only show selected machine IDs** option. (This option was described earlier in **Filtering Machine ID Accounts** *(page 4)*.) For example, if you define a machine ID template called "laptops", then it's easier to apply settings to all the "laptops" you're responsible for if you have a filtered view called "laptops". Simply select the view for "laptops" and only laptops are displayed on any function page, regardless of the machine group they belong to. The same idea applies to "desktops", "workstations", Exchange servers", etc.

Filtered views of selected machines are particularly useful when you're getting ready to copy settings from a machine ID template to existing agents using the **Copy Settings** function described above.

Base Templates and Audits

Since you can never be sure what settings should be applied to a machine until you perform an audit on the machine, consider installing an agent package created from a "base" template that has most of the agent settings *turned off*. Once you have the audit, then you can decide which settings should go on which machine. Use the **Copy Settings** function to copy settings from the appropriate template to the new agent.

Creating Agent Install Packages

Agent Install Packages

Rapid deployment is an important feature of the VSA. Getting the system up and running as quickly as possible helps the IT group get machines under management immediately and allows for the implementation of best practices. One aspect of rapid deployment is the ability to deploy agents that are totally configured using **agent install packages**.

Agent install packages are created using two functions within the VSA:

- **Deploy Agents** - Creates and distributes an agent install package to *multiple* machines. This is the preferred method for creating agent install packages and discussed in detail in this document.
- **Create** - Creates a machine ID account and agent install package in two separate steps. The install package is applied to a *single* machine. You can also use **Create** to create machine ID templates or re-install a missing agent for an *existing* machine ID.

Deploy Agents

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

- Use Agent > Create 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 or re-install an agent for an *existing* machine ID.
- Use Install Agents to install agents *on remote systems*.

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

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 `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 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 ystem 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 and subsequently install agents *remotely* using the Agent > Install Agents 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 and View AD Users. 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.

✓ 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 can only be used when creating the agent install package.
>
> **Note:** For Linux, see Installing Linux Agents 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, 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 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 may be used afterwards, to manually copy specific kinds of agent settings by machine ID template 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 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.
   - **Prompt User** - Asks user to enter a group ID. This option only displays for master role users.
3. Specify agent install package command line switches including the ability to install silently without any task bars or dialog boxes.
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.**

   Note: *Credentials are only necessary if users are installing packages on machines and do not have administrator access to their network.*
7. Name the install package for easy reference later. This name displays on the **Deploy Agents** page and the `dl.asp` download page.

Install Issues and Failures

See Install Issues and Failures 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.

Distributing Agent Install Packages

Download Methods Using Deploy Agent

The **Deploy Agent** page provides three types of links for downloading agent install packages:

- The user's *default* agent install package - Each user has his or her own default agent install package.
- A *selected* agent install package - First, select any package listed in the Deploy Agent page. Secondly, click this link to download this selected package using a unique index number assigned to the package.
- A `dl.asp` web page listing *all publicly available* agent install packages - Click any package listed on the `dl.asp` web page to download it.

Any of these methods downloads the same `KcsSetup` file used to install the agent.

Executing the Install Package

The downloaded KcsSetup can be executed using any of the following three methods:

- Double click KcsSetup to launch it.
- Open a **command line window** and type KcsSetup followed by any desired command line switches. These switches are described in the user guide or online user assistance.
- Select **Run...** from the **Windows Start** menu and type KcsSetup followed by any desired command line switches.

Distribution Methods

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

- **Logon** Procedures - Set up an **NT logon** procedure to run the install package every time a user logs into the network. The installer skips installation if it detects an agent is already on a machine.
  1. Create the deployment package using the Agent > **Deploy Agents** wizard.
  - ✓ 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 KcsSetup 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 KcsSetup, then attach it to an email on your local machine. You can also copy and paste the link of a dl.asp install package into an email message.
- **LAN Watch** - users can discover newly added machines during a LAN Watch and subsequently install agents *remotely* using the Agent > **Install Agents** page. If a LAN Watch is performed using an Active Directory machine, you can also install agents to Active Directory computers using **View AD Computers**. Agents can also be automatically installed on each machine an Active Directory user logs onto using **View AD Users**.
- **Manually** - You can instruct users to download an install package agent from the http://your.Kserver.com/dl.asp website to their target machines. If more than one install package is displayed on the website, instruct them which package should be selected.

Automatic Account Creation

You should be aware that *automatic account creation* is enabled using System > **Check-in Policy** to automatically create a machine ID account when an agent install package is installed. This option is enabled by default when the VSA is installed.

Assigning New Machine IDs to Machine Group by IP Address

You may choose to create a "generic" install package that adds all new machine accounts to the unnamed group ID. When the agent checks in the first time, the System > **Naming Policy** assigns it to the correct group ID and/or sub-group ID using the IP address of the managed machine.

Configuring Agents on an Internal LAN

If machines on an internal LAN cannot be routed to the VSA using the external host name or IP address:

1. Create an agent installation package that copies settings from an existing machine account which has its primary and secondary KServer address set to the server's *internal* IP address. The primary and secondary Kserver addresses are displayed using the **Check-In Control** function underneath the **Agent** tab.
2. If a machine account with this setting does not exist, then create a new machine ID template, with a name such as *default-internal.unnamed*, using the Agent > **Create** page.
3. Set the new account's primary and secondary KServer addresses to the KServer's internal IP address using the **Check-In Control** page.
4. Use **Deploy Agents** to create an installation package based on this machine ID. The installation package can then be deployed to managed machines on the internal LAN.

Agent Functions

Once agents are installed you can maintain them using a variety of additional functions. The complete list of functions provided by the **Agent** module in the VSA includes:

Functions	Description
Agent Status	Displays active user accounts, IP addresses and last check-in times.
Agent Logs	Displays logs of: • Agent system and error messages • Execution of agent procedures, whether successful or failed. • Configuration changes made by a user. • Send/receive data for applications that access the network. • Application, System, and Security event log data collected from managed machine. • Alarm log • Remote control log • Log monitoring
Log History	Specifies how long to store log data.
Event Log Settings	Specifies event log types and categories included in event logs.
Deploy Agents	Creates agent install packages for installing agents on multiple machines.
Create	Creates machine ID accounts and/or install packages for installing agents on single machines.
Delete	Deletes machine ID accounts.
Rename	Renames existing machine ID accounts.
Change Group	Reassigns machines to a different machine group or subgroup.

LAN Watch	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.
Install Agents	Installs the agent *on a remote system* and creates a new machine ID / group ID account for any new PC detected by LAN Watch.
View LAN	Displays the results of the latest LAN Watch scan.
View AD Computers	Lists all computers listed in an Active Directory when LAN Watch runs on a system hosting Active Directory. Installs agents on AD machines.
View AD Users	Lists all Active Directory users discovered by LAN Watch when LAN Watch runs on a system hosting Active Directory. Creates VSA users from AD users.
View vPro	Displays hardware information about vPro-enabled machines discovered while running LAN Watch.
Copy Settings	Mass copies settings from one machine account to other machine accounts.
Import / Export	Imports and exports agent settings, including scheduled agent procedures, assigned monitor sets, and event sets, as XML files.
Suspend	Suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings.
Agent Menu	Customizes the agent menu on managed machines.
Check-In Control	Controls agent check-in frequency on agent machines.
Working Directory	Sets the path to a directory used by the agent to store working files.
Edit Profile	Edits machine account information.
Portal Access	Sets up accounts to allow machine users remote control access to their own machines.
Set Credential	Sets a logon credential for the agent to use in Patch Management, the Use Credential procedure command, Endpoint Security, and Desktop Policy and Migration.
Update Agent	Updates the agent software on managed machines.
File Access	Prevents unauthorized access to files on managed machines by rogue applications or users.
Network Access	Lets you approve or deny network access on a per application basis.
Application Blocker	Application blocker prevents any application from running on a managed machine.

Summary

The following agent configuration and deployment summary incorporates "best practices" recommendations discussed throughout this document.

Planning

After reviewing this document and before you deploy agents, a plan should be created that identifies how the machines will be managed on a daily, weekly and monthly basis. This helps determine how they should be grouped. Although it is very easy to reassign a machine to a group or sub group, planning will help with a rapid and smoother deployment. In addition, user security can be defined to restrict group access.

- **Users**
  - Identify users and end users.
  - What access do they need?
- **Organizations, Group and Sub-Groups**
  - What named grouping is needed? By department, location, client, location, user type, etc.
- **Reporting**
  - What is the granularity by organization, group, sub-group, and view?
  - Who gets the reports? Who are the internal and external recipients?

Machine ID Templates and Filtered Views

- Identify the different types of machines you'll be required to support.
- Create additional machine ID templates, one for each type of machine you have identified.
- Create corresponding filtered views for each type of machine.
- Create a "base" machine ID template with most of the agent settings turned off.

Agent Configuration

Define and create agent settings, as appropriate, for each machine ID template you have defined. You don't have to have all these settings defined initially. You can update a template, then copy the template's settings to working agents repeatedly using the **Copy Settings** function. Be sure to select "Do Not Copy" for any agent settings you do not want to overwrite.

Package Creation

Use the package wizard in Agent > **Deploy Agent** to create the agent package to install. Use a machine ID template as the source of agent settings for the package.

Consider installing an agent based on a "base" template with most of the agent settings *turned off*. Once the package is installed on a new machine, review the audit for a newly managed machine first, then apply settings from the appropriate template to the new agent as appropriate using the **Copy Settings** function.

Consider *automating* the assignment of managed machines to groups and subgroups using the System > **Naming Policy** function.

Deployment

Identify locations, types of users, and machine availability. These factors determine the need for one or more methods of deployment. A domain login procedure is the quickest. However, not all environments use domains. **LAN Watch** only works with NT and higher. If you have a domain and are using Active Directory, consider using Active Directory to identify machines that should have agents installed. Remember installs can be silent and require no user interaction or reboot.

Agent Reconfiguration

When you need to reconfigure agents, make your changes to the appropriate machine ID templates first. This ensures your machine ID templates remain the "master repositories" of all your agent settings. Then filter your view of all the machines you're responsible for, by selecting a view of selected machines that corresponds to the template you have modified. Use **Copy Settings** to copy settings from your modified template to *all* the machines in your *filtered view*. Be sure to select "Do Not Copy" for any agent settings you do not want to overwrite.

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.