Kaseya 2

Directory Services

User Guide

Version 1.0

May 3, 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

Directory Services Overview 1

- KDS System Requirements 1
- Licensing 2
- Getting Started 2
  - Managing a Synchronized Security Model 3
  - Managing Multiple Domains 3
  - Managing Remote Portal Access 4
- Setting KDS Policies 4
  - Setting KDS Policies for Computers 5
  - Setting Policies for Computers 5
  - Setting KDS Policies for Users 5
- Applying KDS Policies 6
  - How Agents are Installed Using KDS 6
  - How Machine ID Accounts are Created in KDS 7
  - How Machine Moves in Domains are Reflected in KDS 7
  - Enabling Remote Portal Access in KDS 8
  - Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords 9
  - Making Changes to KDS Managed User Logons 9
- Synchronization 10
- Deactivation / Reactivation 11
- Uninstalling 12
- Probe Alerts and Domain Alerts 12
- Configuring the KDS Domains Page 12
  - Configuration Prerequisites 12
  - Configuring Probe Deployment 13
  - Configuring Agent Deployment Policy 14
  - Configuring Computer Policies 14
  - Configuring Contact Policies 15
  - Configuring User Policies 16
  - Configuring Alert Policies 17
  - Configuring Schedule and Status 17

Computers 18

Contacts 19

Users and Portal Users 21

Domains 25

- Probe Deployment 26
- Agent Deployment Policy 27
- Computer / Contact Policies 28
- User Policies 29
- Alert Policies 31
- Schedule and Status 32

Audit Log 33
Glossary of Terms 35
Index 39

Directory Services Overview

Directory Services (KDS) installs agents on newly discovered Active Directory domain machines and manages VSA user logons and Portal Access logons using domain logons. KDS can also create staff records based on contacts in the domain. Changes in the domain are synchronized with KDS on a scheduled basis and do not require a VSA agent on the AD domain controller. KDS uses the industry standard LDAP protocol to safely and securely communicate with Active Directory domains.

Directory Services:

- Automatically discovers AD domains that can be synced with the VSA.
- Automatically creates a VSA security hierarchy modeled after an existing domain hierarchy.
- Automatically keeps the VSA synchronized with all domain changes.
- Automatically creates VSA users and staff member records in the VSA based on the creation of users and contacts in the domains.
- Auto-populates domain user and contact information in Service Desk tickets.
- Auto-deploys agents to domain computers. Agents are automatically placed in the appropriate machine group relative to the domain hierarchy.
- Resets a domain password or enable/disables a domain user from the VSA.

Note: *See* **KDS System Requirements** *(page 1).*

Functions	Description
Computers *(page 18)*	Manages machine ID accounts created, based on applied KDS computer policies, for all domains monitored by KDS probes.
Contacts *(page 19)*	Manages staff records created, based on applied KDS contact policies, for all domains monitored by KDS probes.
Users and Portal Users *(page 21)*	Manages VSA users and Portal Access candidates created, based on applied KDS group policies, for all domains monitored by KDS probes.
Domains *(page 25)*	Configures the integration of KDS with Active Directory domains.
Audit Log *(page 33)*	Displays a log of KDS module activities.

KDS System Requirements

KServer

- The Directory Services module installs on VSA 6.1 or later

Note: *See general System Requirements.*

Requirements for Each KDS Managed Machine

- Windows OS: XP, Vista, Server 2003, Server 2003 R2, Server 2008, Server 2008 R2, or Windows 7
- Installing probes and installing agents on Mac and Linux computers using KDS are not supported. If Linux and Mac computers are located in the Domain hierarchy, these computers can be identified using KDS and agents can be installed on them manually outside of KDS.

Licensing

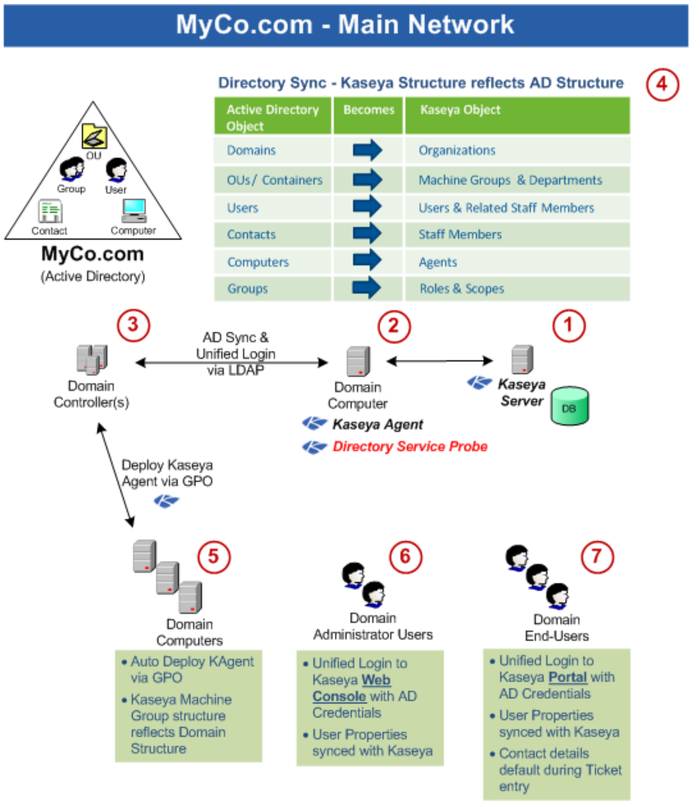
Directory Services is licensed by the number of KDS managed domains. A managed domain is a domain attached to an organization. A domain is attached to an organization when *activated* using the Domains > **Probe Deployment** *(page 26)* tab. Directory Services can be in one of following licensing states:

- **Unlicensed** - KDS is installed and visible in the VSA but zero domains are licensed.
- **Licensed** - A sufficient number of licenses exist for the domains being managed.
- **Exceeded** - Another domain cannot be installed, because the maximum number of domains has been installed.
- **Expired** - KDS has been disabled because licensing for the entire module has expired.

Getting Started

KDS on the Kserver (1) uses a probe agent on a domain computer (2) to communicate with an Active Directory domain (3). Once connected, the probe "harvests" domain data (4) back to the Kserver.

- Agents are deployed to domain machines using a group policy object (GPO) to download the agent install package (5).
- VSA users can use their domain credential to logon to the VSA (6).
- Portal Access users can use their domain credentials to logon remotely to their machines (7).



Active Directory Object	Becomes	Kaseya Object
Domains	➡	Organizations
OUs/ Containers	➡	Machine Groups & Departments
Users	➡	Users & Related Staff Members
Contacts	➡	Staff Members
Computers	➡	Agents
Groups	➡	Roles & Scopes

- Auto Deploy KAgent via GPO
- Kaseya Machine Group structure reflects Domain Structure

- Unified Login to Kaseya **Web Console** with AD Credentials
- User Properties synced with Kaseya

- Unified Login to Kaseya **Portal** with AD Credentials
- User Properties synced with Kaseya
- Contact details default during Ticket entry

The following topics provide a step-by-step procedure for configuring KDS.

- **Domains Page Prerequisites** *(page 12)*
- **Configuring Probe Deployment** *(page 13)*
- **Configuring Agent Deployment Policy** *(page 14)*
- **Configuring Computer Policies** *(page 14)*
- **Configuring Contact Policies** *(page 15)*

- **Configuring User Policies** *(page 16)*
- **Configuring Alert Policies** *(page 17)*
- **Configuring Schedule and Status** *(page 17)*

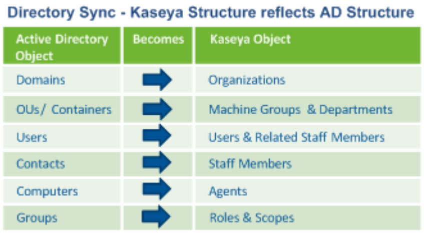
These additional topics provide an overview of KDS concepts.

- **Managing a Synchronized Security Model** *(page 3)*
- **Managing Multiple Domains** *(page 3)*
- **Managing Remote Portal Access** *(page 4)*
- **Setting KDS Policies** *(page 4)*
- **Applying KDS Policies** *(page 6)*
- **Synchronization** *(page 10)*
- **Deactivation / Reactivation** *(page 11)*
- **Probe Alerts and Domain Alerts** *(page 12)*

Managing a Synchronized Security Model

One of the benefits of synchronizing the VSA with the domain is that the domain hierarchy of folders and items—domains, organizational units/containers, computers, groups, users, and contacts—is automatically "harvested" to create and maintain a similar security model in the VSA—organizations, machine groups, machines, users, scopes, roles, and staff. Service providers are freed from having to enter the same data a second time in the VSA. For example, user data, such email, phone and other contact information need only be updated in the domain to update corresponding fields in the VSA.

The security model created in the VSA by KDS integration with the Active Directory domain results in the following mapping of objects.

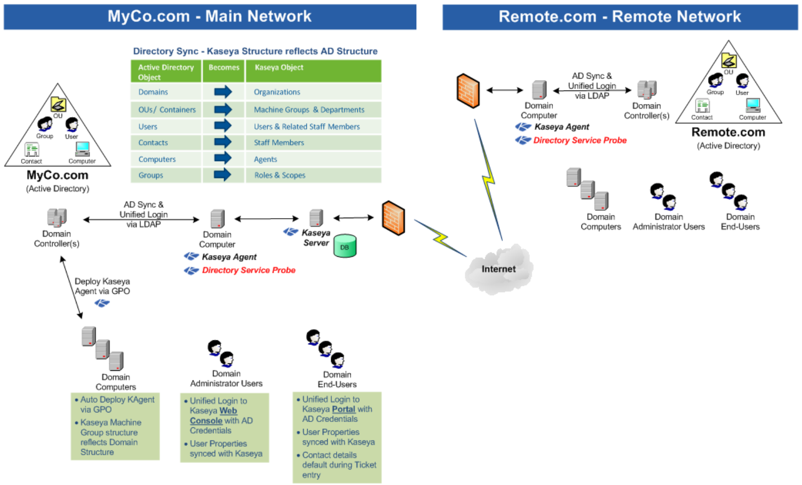


Directory Sync - Kaseya Structure reflects AD Structure

Active Directory Object	Becomes	Kaseya Object
Domains	➡	Organizations
OUs/ Containers	➡	Machine Groups & Departments
Users	➡	Users & Related Staff Members
Contacts	➡	Staff Members
Computers	➡	Agents
Groups	➡	Roles & Scopes

Managing Multiple Domains

KDS provide consolidated access throughout the VSA to KDS managed domain computers, users and contacts, regardless of whether these domains have a "trust" relationship between them. For example, KDS can provide a consolidated view of the domains of both a primary company and a subsidiary company.

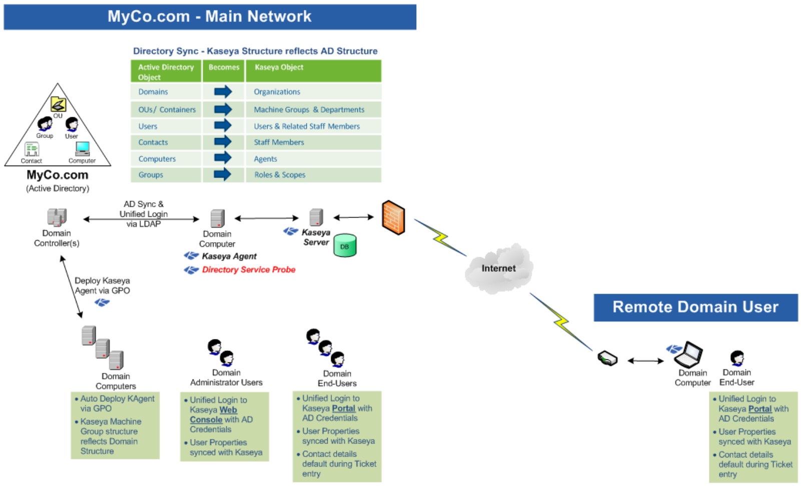

MyCo.com - Main Network
Remote.com - Remote Network
Directory Sync - Kaseya Structure reflects AD Structure
OU
Group
User
Contact
Computer
MyCo.com
(Active Directory)
AD Sync &
Unified Login
via LDAP
Domain
Controller(s)
Domain
Computer
Kaseya Agent
Directory Service Probe
Kaseya
Server
DB
Deploy Kaseya
Agent via GPO
Domain
Computers
Domain
Administrator Users
Domain
End-Users
• Auto Deploy KAgent via GPO
• Kaseya Machine Group structure reflects Domain Structure
• Unified Login to Kaseya Web Console with AD Credentials
• User Properties synced with Kaseya
• Unified Login to Kaseya Portal with AD Credentials
• User Properties synced with Kaseya
• Contact details default during Ticket entry
Internet
Remote.com
(Active Directory)

Active Directory Object	Becomes	Kaseya Object
Domains	➡	Organizations
OUs/ Containers	➡	Machine Groups & Departments
Users	➡	Users & Related Staff Members
Contacts	➡	Staff Members
Computers	➡	Agents
Groups	➡	Roles & Scopes

- Each KDS managed domain is associated with a unique organization within the VSA.
- A scope matching the name of the organization is created. If you like you can add multiple organizations to the same scope. This enables a VSA user to use a single scope to have visibility of all machine groups in multiple organizations.
- The machine ID / group ID filter enables you to filter the display of machines—by machine property, machine group or organization.

Managing Remote Portal Access

KDS sets policies that enable users to use their domain credentials to logon remotely to their machines use Portal Access. Remote access using Portal Access can be inside or outside of the company's firewall. For example, a Portal Access user might want to access their office computer from home.


MyCo.com - Main Network
Directory Sync - Kaseya Structure reflects AD Structure
OU
Group
User
Contact
Computer
MyCo.com
(Active Directory)
AD Sync &
Unified Login
via LDAP
Domain
Controller(s)
Domain
Computer
Kaseya Agent
Directory Service Probe
Kaseya
Server
DB
Deploy Kaseya
Agent via GPO
Domain
Computers
Domain
Administrator Users
Domain
End-Users
• Auto Deploy KAgent via GPO
• Kaseya Machine Group structure reflects Domain Structure
• Unified Login to Kaseya Web Console with AD Credentials
• User Properties synced with Kaseya
• Unified Login to Kaseya Portal with AD Credentials
• User Properties synced with Kaseya
• Contact details default during Ticket entry
Internet
Remote Domain User
Domain
Computer
Domain
End-User
• Unified Login to Kaseya Portal with AD Credentials
• User Properties synced with Kaseya
• Contact details default during Ticket entry

Active Directory Object	Becomes	Kaseya Object
Domains	➡	Organizations
OUs/ Containers	➡	Machine Groups & Departments
Users	➡	Users & Related Staff Members
Contacts	➡	Staff Members
Computers	➡	Agents
Groups	➡	Roles & Scopes

Setting KDS Policies

Once a probe is installed, KDS is configured by setting selected domain folders and items to **included** or **excluded**. KDS policies provide IT automation—such as installing agents or creating users—only for *included* folders and items. KDS only harvests detailed information for *included* folders and items, minimizing the amount of data required to maintain synchronization with the domain.

KDS policies can be set for three types of domain objects:

- **Setting KDS Policies for Computers** *(page 5)*
- **Setting KDS Policies for Contacts** *(page 5)*

- **Setting KDS Policies for Users** *(page 5)*

Setting KDS Policies for Computers

The following KDS computer policies can be set for each OU/container in the domain.

- Automatic deployment of agents on newly discovered machines
- Manual deployment of agents on selected machines
- Agent deployment on the system hosting the Active Directory domain
- Designating all machines or selected machines as **portal candidates** *(page 8)*.

Creating a machine ID account using a KDS policy also creates a machine group hierarchy for the new machine ID account that reflects the OU/container hierarchy in the domain.

KDS computer policies are set using the **Computer / Contact Policies** *(page 28)* tab of the **Domains** page.

Setting Policies for Computers

The following KDS *contact* policies can be set for each OU/container in the domain.

- Automatic creation of VSA staff records for all newly discovered domain contacts
- Manual creation of VSA staff records for all selected domain contacts in an OU/container

Creating a staff record using a KDS policy also creates a hierarchy of departments that reflects the OU/container hierarchy in the domain.

KDS contact policies are set using the **Computer / Contact Policies** *(page 28)* tab of the **Domains** page.

Setting KDS Policies for Users

KDS can create VSA users and Portal Access users based on domain users. This means IT administrators can provide their users the same credential for these applications and manage authentication and authorization from a single location, using the Active Directory domain.

The following KDS *user* policies can be set for each (user) group in the domain. These policies are applied to all users belonging to the group. They cannot be applied to individual users within a group.

1. `Do Not Include Users` - Do not create VSA user logons or Portal Access logons for domain users listed in this user group.
2. `Create Staff Members` - Creates a staff member record. These users can be assigned Portal Access to a machine *manually*.
3. `Create Staff and make Auto Portal Candidates` - Designates domain users in this user group as Portal Access candidates. See **Making Portal Access Candidates** *(page 8)* for details.
4. `Create VSA Users` - Creates VSA user logons for domain users listed in this group.
   - ➢ If `Create VSA Users` is selected, a scope and role must be selected for that user group. You can optionally create a new scope.

Since each domain user can belong to multiple domain user groups, a domain user is assigned the **highest ranking VSA logon policy** *assigned to any user group the domain user is a member of.*

- `Create VSA Users` outranks `Create Staff and make Auto Portal Candidates`
- `Create Staff and make Auto Portal Candidates` outranks `Create Staff Members`
- `Create Staff Members outranks` outranks `Do Not Include Users`

> **Note:** A domain user can only be associated with either VSA user logon or a Portal Access logon, but not both at the same time. See **Making Changes to KDS Managed User Logons** *(page 9)*.

KDS user policies are set using the **User Policies** *(page 29)* tab of the **Domains** page.

Applying KDS Policies

Once all KDS policies are set, the settings are applied. Several minutes later, new VSA computers, contacts, VSA users and Portal Access users display in their respective KDS pages in the following KDS page, depending on the KDS policies that were applied.

- **Computers** *(page 18)*
- **Contacts** *(page 19)*
- **Users and Portal Users** *(page 21)*

Review the following specialized topics to ensure you understand how these new VSA records are created and what additional configuration tasks may be required for each type of VSA record created using KDS.

- **How Agents are Installed Using KDS** *(page 6)*
- **How Machine ID Accounts are Created in KDS** *(page 7)*
- **How Machine Moves in Domain are Reflected in KDS** *(page 7)*
- **Enabling Remote Portal Access in KDS** *(page 8)*
- **Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords** *(page 9)*
- **Making Changes to KDS Managed User Logons** *(page 9)*

How Agents are Installed Using KDS

All agents installed on domain machines using KDS are installed using a single agent install package specified for each domain.

Since different types of machines may require different agent settings, Kaseya recommends specifying a "generic" agent install package for KDS agent installs. Change the agent settings after the install, as appropriate, for each type of machine. Agent settings can be changed manually using machine ID templates and Agent > Copy Settings or by importing agent settings using Agent > Import / Export.

KDS uses two method for installing agents. Both methods are initiated simultaneously when KDS deploys an agent to a machine. An installed agent cancels additional attempts to install the agent.

Method 1 - Agent Installs Using Kconnect

This method is successful most of the time and installs the agent immediately without requiring a reboot of the machine. It is the same technology used by LAN Watch to remotely install an agent. The agent install package is downloaded from the KServer to the agent probe computer. The agent probe computer runs a Kaseya utility called `Kconnect.exe`. The agent probe machine uses its Active Directory domain credential to transfer the file to the target computer and install the agent.

Method 2 - Agent Installs using a GPO Script

This method does not occur until the target computer is rebooted. A single copy of the agent install package for each domain is stored on the system hosting the Active Directory domain. A Group Policy Object (GPO) is created for the domain in Active Directory. When an agent is deployed using KDS the GPO is assigned to that domain machine in Active Directory. If an agent is not already installed on the domain machine, the GPO triggers an agent install the next time the domain machine is rebooted. *If the agent is deleted from the domain machine, the GPO method of installing the agent ensures that the agent is re-installed.*

The copy of the agent install package on the system hosting the Active Directory domain is *not* automatically updated when the agent install package is changed. For this release, to update the agent install package manually:

1. In Active Directory, locate the Features > Group Policy Management > <forest> > Domains <domain> > **Group Policy Objects** folder.
2. Right-click the **ADAgentDeployGPO** group policy object and select the **Edit...** option to open the **Group Policy Management Editor** dialog.

3. Locate the Computer Configuration > Policies > Windows Settings > Scripts folder.
4. Right-click the **Startup** script and select the **Properties** option to open up the **Startup Properties** dialog.
5. Select the **InstallAgent.vbs** script and click the **Show Files...** button to display a Windows explorer window.
6. A `KcsSetup<number>.exe` file displays in the selected file folder with a unique number added to the end of the filename. For example: `KcsSetup35475311.exe`.
7. Rename the old `KcsSetup<number>.exe` file and replace it with your updated `KcsSetup.exe`.

> **Note:** Ensure you rename the `KcsSetup.exe` file to the exact `KcsSetup<number>.exe` filename that was used before, including the unique number that was previously used.

New installs of the agent using the GPO method will now install using the agent settings in the new agent install package.

> **Note:** When installing an agent to a Windows XP domain machine using the GPO method, installs may fail if the **Security Center domain policy is disabled** (**http://technet.microsoft.com/en-us/library/cc725578(WS.10).aspx**).

How Machine ID Accounts are Created in KDS

The creation and grouping of **machine ID accounts** *(page 36)* using KDS depends on how machines are organized in the domain and whether the machine ID accounts already exist in the VSA.

- A single organization is specified for each domain in KDS. The organization selected determines the organization assigned to *newly created machine ID accounts* when installed using KDS.
- The appropriate hierarchy of machine groups for a new machine ID account are created, if the machine group hierarchy doesn't already exist, matching the machine's location in the OU hierarchy in the domain.
- Newly created machine ID accounts initially display as "empty" machine ID template accounts—identified with a ▣ check-in icon—meaning there is no corresponding agent for this machine ID account.
- If no *agent* exists on the domain machine, then a new agent is installed after a reboot of the computer using the newly created machine ID account.
- If an agent already exists on a managed machine in a different machine group, then KDS creates an "empty" **machine ID template** *(page 36)* account—identified with a ▣ check-in icon—and no agent ever checks in. The new machine ID template account displays a **machine.ID / group ID / organization ID** *(page 36)* based on the computer's canonical name in the Active Directory domain. *You can merge these duplicate accounts.* The existing, active agent account adopts the name of the new machine ID template account, then the new machine ID template account is deleted. No data is lost by the merge and the machine ID account now matches its location in the domain hierarchy.
- Select a **Duplicate Exists** row in the Directory Services > **Computers** *(page 18)* page then click the **Merge Duplicates** button.

> **Warning:** Use the **Merge Duplicates** method to merge duplicates rather than merging accounts using the Agent > Rename page.

How Machine Moves in Domains are Reflected in KDS

When a machine is *moved* to a new OU in the domain, the effect it has in KDS depends on the policies selected using the Directory Services > Domain > **Computer / Contact Policies** *(page 28)* tab. KDS monitoring of a member machine in the domain depends on whether its policy is set to "included" or "excluded" in both the source OU location and the target OU location.

Assuming the `Include New Computers` checkbox is checked in the target location:

- **From Included to Included** - The machine ID account hierarchy is changed to match the new location in the domain hierarchy.
- **From Included to Excluded** - The machine ID account hierarchy is not changed. The VSA must move the machine ID manually using Agent > Change Group.
- **From Excluded to Included** - A new "empty" machine ID account hierarchy is created, matching the new location in the domain hierarchy. The VSA user can choose to merge the old machine ID account with the newly created machine ID account using the Directory Service > Computers > **Merge Duplicates** button.
- **From Excluded to Excluded** - No change is made in the VSA.

Enabling Remote Portal Access in KDS

When a domain user logs on to a domain machine, *both the domain machine and the domain user* must be designated as KDS **portal candidates** to enable the user to be *automatically assigned* as the Portal Access user of that machine. KDS can also manually assign and remove Portal Access for domain users, regardless of whether the domain user or domain computer is a portal candidate or not.

> **Note:** A domain user can be either a VSA user or a Portal Access user but not both. Once a VSA user logon has been created for a domain user, that user is no longer eligible to be a Portal Access user of any machine.

For more information see:

- **Managing Remote Portal Access** *(page 4)*

KDS managed Portal Access provides the following unique behavior not available outside of KDS.

- When a portal candidate user logs on to a portal candidate machine—and that portal candidate machine is not already assigned a Portal Access user—he or she is automatically assigned the Portal Access user of that machine.
- The **Change Profile** tab of Portal Access is automatically populated with the *name*, *email* and *phone number* of the currently logged in Portal Access candidate. The submitter fields of new **Service Desk** tickets are populated with the contact information stored in the **Change Profile** tab. This means Portal Access users don't have re-enter the same contact information, each time they create a new **Service Desk** ticket.

  > **Note:** Regardless of the submitter information recorded in a ticket, the current Portal Access user sees all tickets related to that machine.

- If connection to the Active Directory server is lost, preventing domain authentication, users can still use their Portal Access logon to logon remotely to the Portal Access machine they were last assigned.
- All machines can be designated portal candidates using the **Automatically assign portal access to portal candidates** checkbox in the Computers Policy dialog on the **Computer / Contact Policies** *(page 28)*. tab.
- Any domain user who is not already a VSA user—whether a portal candidate or not—can be manually assigned the Portal Access user of a domain computer, using the **Assign Portal User** button on the **Computers** *(page 18)* page.

  > **Note:** The user must have logged on to a machine at least once, and no one else can be currently assigned to that machine as the Portal Access user.

- Any domain user—whether a portal candidate or not—can be manually removed as the Portal Access user of any domain computer at any time, using the **Remove Portal User** button on the **Computers** *(page 18)* page.

Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords

When the KDS > Users and Portal Access page is used to enable or disable a domain user account or reset a domain user's password, synchronization occurs immediately for only that domain user record. Detailed domain data is harvested for only that domain user.

- A disabled domain user will no longer be able to logon using the domain credential, nor be able to logon to the VSA using their domain credential.
- Password changes take effect the next time the domain user logs on, to both the domain and to the VSA using their domain credential.

> **Note:** Enabling/disabling domain user accounts or resetting domain user passwords *in Active Directory* will not update the VSA until a read time synchronization occurs.
>
> **Note:** Do not make changes to the password of a KDS managed user or enable/disable that user using the System > Users page or System > Change Logon page. These changes *only occur in the VSA* and only have a temporary effect on that user. Eventually synchronization will reset the user's VSA password and enable/disable the VSA user as specified in Active Directory.

Making Changes to KDS Managed User Logons

You may wish to make changes to created VSA user logon or Portal Access candidates after applying KDS policies. You should be aware that:

- The VSA users and Portal Access users created by KDS are never removed automatically by KDS.
- The agents installed by KDS are never uninstalled by KDS.

The deletion of VSA users and Portal Access users and the uninstalling of agents must always be made manually, outside of KDS.

> **Note:** An domain user can only be associated with *either* a VSA user logon *or* a Portal Access logon, *but not both at the same time.*

Removing VSA User Logon Access Only

- Delete the VSA user logon only.

Removing Portal User Access Only

- Use the Remove Portal Users button on the User and Portal Access page.

Promote a Portal Access Candidate to a VSA User

- Use the Remove Portal Users button on the User and Portal Access page.
- Modify KDS policies so that at least one group the domain user belong to is set to `Create VSA User`. The <VSA user will be created when the KDS user policy is applied.

Demote a VSA User to a Portal Access User

- Delete the VSA user logon only.
- Modify KDS policies so that at least one group the domain user belong to is set to `Create Staff and make Auto Portal Candidate` and no groups the domain user belongs to are set to `Create VSA user`. The Portal Access candidate will be created when the KDS user policy is applied.

Synchronization

Synchronization refers to the updating of KDS with data harvested from an Active Directory domain. The following KDS events trigger synchronization between KDS and a domain.

- Previews
- Activation / Incremental Synchronization
- Apply Changes
- Full Synchronization

> **Note:** *A synchronization also occurs for a specified user when* **Enabling/Disabling Domain Users Accounts or Resetting Domain User Password** *(page 9).*

Previews

When the KDS probe is installed, the first task the probe performs is a **preview**. A preview updates KDS with:

- Summary domain data for all folders and items.

Since this is the first time data is "harvested" from a domain, only summary domain data is required.

- Folders are domain objects that contain other objects. This can refer to organizational units or containers, and groups, meaning groups of users.
- Items can refer to computers, users and contacts.

Activation / Incremental Synchronization

After the probe is installed, —and typically before KDS policies are even set—a KDS probe is activated. **Activation** enables incremental synchronization between an Active Directory domain and the probe computer. An activated probe waits a fixed period of time, call the **synchronization interval**, before updating the VSA with these changes. By default this synchronization interval is 60 minutes. If this default value is used, these domain changes may not be reflected in the VSA up to 60 minutes after the changes are made.

Initially no KDS policies have yet been set, so no folders or items are "included", which would require a detailed harvesting of data. In this case an incremental synchronization harvests summary data from a domain that is similar to a preview, except the harvesting of data is limited to *changes* in the domain.

Later, when KDS policies have been set and selected folders and items are "included," synchronization requires both summary and detailed data. Again the harvesting of data is limited to *changes* in the domain.

Incremental synchronization provides an update of *all changes* to:

- Summary domain data for all folders and items, whether "included" or "excluded"
- Detailed domain data for all "included" folders and "included" items. Computers and contacts can be "included" individually. Users are always "included" by group.

Domain Changes Using the Incremental Synchronization Interval

Most domain changes are stored by the probe until the synchronization interval has elapsed, then uploaded to KDS. The default is 60 minutes. These types of domain changes include:

- User added, moved or deleted
- Computer added, moved or deleted
- User or contact changes such as name, address, phone number, email address
- Reorganization of the domain OU hierarchy

Domain Changes Passed Immediately

A few important domain changes need to be uploaded by the probe immediately. These include:

- Password changes

- Disabling a user account

Apply Changes

Synchronization also occurs when **applying KDS policies** *(page 6)*, and are equivalent to a *full* synchronization. This ensures applied policies affect *all* **included** *(page 35)* domain computers, users and contacts that may exist at that time, regardless of any synchronizations that may have occurred before.

Full Synchronization

The KDS probe accumulates domain *changes* in real time. If the connection between the KDS probe and a domain is lost for a period of time, the probe has no way to recover those changes. To ensure domain changes are not lost forever, set **probe alerts** *(page 12)* and schedule a recurring *full* **synchronization** *(page 10)*. *If a probe alert is triggered, consider running a full synchronization immediately.*

A full synchronization provides KDS with a complete update of domain data, including:

- Summary domain data for all folders and items, whether "included" or "excluded"
- Detailed domain data for all "included" folders and "included" items. Computers and contacts can be "included" individually. Users are always "included" by group.

Typically full synchronization occurs less frequently than incremental synchronization. Once a day or once a week, for example, might be sufficient.

Deactivation / Reactivation

Deactivation

Once activated, a KDS probe can be deactivated. There are two types of deactivation.

- **Deactivation**
- **Deactivation and Detaching the Org**

Deactivation alone stops the probe from receiving incremental synchronization updates from the domain. If reactivation occurs later, a "changes gap" may exist in the data collected by the probe, requiring the scheduling of a full synchronization to correct.

Deactivation and Detaching the Org

If the wrong organization is associated with the domain, you can deactivate the probe *and detach the organization* selected for the domain. Deactivating and detaching the organization does not uninstall the probe.

Deactivating and detaching the org clears all records for that domain in the **Computers** *(page 18)*, **Contacts** *(page 19)* and **Users and Portal Users** *(page 21)* pages, because these records are no longer known to be members of the domain by way of the org association. The actual VSA records are not deleted. Detaching the org also does not delete any preview information or policy information obtained by the probe. All of this remains available to the probe even when the probe is not activated and an organization has not yet been selected for the domain.

Reactivation

You can select a different organization for the domain and reactivate the probe. New machine ID accounts will be created for the newly selected organization. If any machine ID accounts exist for the previously selected organization, these can be merged using the **Merge Duplicates** button on the **Computers** *(page 18)* page.

> **Note:** Activating a probe on a domain computer *deactivates* any other probe on that same domain, without loss of data.

Uninstalling

Before uninstalling the KDS module from the VSA be sure to deactivate and detach the organization, then uninstall the probe agent.

Probe Alerts and Domain Alerts

Probe Alerts

Probe warnings alerts and failure alerts provides alerts and email notifications for any issues concerning the probe's communication with the Active Directory server. Probe alerts can include:

- The Active Directory server goes offline.
- The domain credential used by KDS is no longer valid.
- The probe cannot communicate with the domain controller.

> **Warning:** The KDS probe accumulates domain *changes* in real time. If the connection between the KDS probe and a domain is lost for a period of time, the probe has no way to recover those changes. To ensure domain changes are not lost forever, set **probe alerts** *(page 12)* and schedule a recurring *full* **synchronization** *(page 10)*. *If a probe alert is triggered, consider running a full synchronization immediately.*

Domain Alerts

Domain alerts provides alarm, ticket and email notifications for create, change and deletes of selected types of objects in the domain. Types of domain objects include:

- Computer
- Contact
- Container
- Domain
- Group
- Organizational Unit
- User

Configuring the KDS Domains Page

The following topics provide a step-by-step procedure for configuring the KDS > **Domains** *(page 25)* page.

- **Configuration Prerequisites** *(page 12)*
- **Configuring Probe Deployment** *(page 13)*
- **Configuring Agent Deployment Policy** *(page 14)*
- **Configuring Computer Policies** *(page 14)*
- **Configuring Contact Policies** *(page 15)*
- **Configuring User Policies** *(page 16)*
- **Configuring Alert Policies** *(page 17)*
- **Configuring Schedule and Status** *(page 17)*

Configuration Prerequisites

1. Identify the domain administrator credentials for the Active Directory domain you intend to integrate with the VSA. KDS requires a domain credential authorized to perform the following types of updates:

- Create a GPO for the purpose of storing Kaseya install packages
- Reset a password
- Enable or disable a user account

> **Note:** A domain administrator credential provides the necessary authorization but you may want to limit KDS to just the privileges listed above.

2. Install a VSA agent on a machine that is a member of the Active Directory domain you intend to integrate with the VSA. You won't see a domain in the upper panel of the **Domains** *(page 25)* page until at least one domain computer has an agent installed on it.

Configuring Probe Deployment

1. Click the Directory Services > Domains > **Probe Deployment** *(page 26)* tab.
2. Select the row of the **Domain Name** in the upper pane you want to configure.
   - The **Probe Status** displays ⊜ `Un-installed`.
   - Machines that are members of this domain and that have Kaseya agents installed on them now display in the lower pane.
   - Initially you may only see a single domain computer with a Kaseya agent installed on it displayed in the lower pane. As agents are automatically installed on other domain computers using KDS policies, these domain computers will all be displayed in the lower pane.
3. Select one of the machines in the lower pane.
   - Click the enabled **Install** button in the lower pane.
4. The first thing the **Install** dialog asks you to enter is a credential. KDS requires a domain credential authorized to perform the following types of updates:
   - Create a GPO for the purpose of storing Kaseya install packages
   - Reset a password
   - Enable or disable a user account

   > **Note:** A domain administrator credential provides the necessary authorization but you may want to limit the KDS to just the privileges listed above.

   After the credential has been verified, the dialog displays a second **Install** button.
5. Click the **Install** button in the dialog. The dialog closes.
   - KDS probe components are installed on the agent machine.
   - After the install, the probe agent automatically begins "harvesting" a **preview** of all *folders and items* in the domain concerning the OU/container hierarchy, computers, contacts, groups and users. No detailed information is requested. The preview populates the **Computer / Contact Policies** tab and **User Policies** tab with this summary data.
   - The **Probe Status** displays ● `Previewing` while harvesting the data. This can take several minutes. Use the **Refresh** button to update the page. Refreshing of the page is not done automatically.
   - When the preview is complete, the **Probe Status** icon displays ◉ `Installed`.
6. Click the **Activate** button in the lower pane. The **Activate Probe** dialog opens.
   - At this point you can enter a different credential for the probe than the one entered for the install. Typically the same credential is used.
   - Specify a **unique** VSA organization for each domain integrated with KDS.
   - ✓ When agents are installed on machines for this domain, the machine ID accounts created in the VSA become members of this organization.
   - ✓ When user records or staff records are created in the VSA for this domain, they are

associated with the organization you select.

- Set a **incremental synchronization interval** *(page 10)* for synchronization of data between the domain and KDS The default is 60 minutes.
- Click the **Activate** button to close this dialog and activate the probe. This should only take a minute or two. Use the **Refresh** button to update the page. Refreshing of the page is not done automatically.
- The **Probe Status** displays ✓ `Activated`.

> **Note:** *Activation is recommended immediately after installing the probe, even before you set additional KDS policies. This ensures all changes in the domain are monitored while you continue with your configuraiton.*
>
> **Note:** See **Deactivation / Reactivation** *(page 11)* for issues to consider before *deactivating* a probe.

Configuring Agent Deployment Policy

1. Click the Directory Services > Domains > **Agent Deployment Policy** *(page 27)* tab.
2. Click the **Edit** button. Set the following:
   - **Automatically install Agents when computer is discovered - Leave this checkbox blank if you have just activated the probe for the first time. Wait until policies are applied, then return to this tab and check this checkbox.** When policies are applied, agents are automatically installed on computers that are members of those policies. *The computers must be rebooted to complete the installation of Kaseya agents.*
   - **Allow Agents to be installed on Directory Server** - Leave this checkbox blank. If checked, agents will also be installed on the system hosting the Active Directory domain.
   - **Default Package** - Select the agent install package to use with the selected domain. See **How Agents are Installed Using KDS** *(page 6)*
3. Click the **Save** button to close this dialog.

Configuring Computer Policies

1. Click the Directory Services > Domains > **Computer / Contact Policies** *(page 28)* tab.
   - Use this tab to specify which domain machines you want to install a Kaseya agent on.
   - Each OU/container in this tab is identified by its canonical name. A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
   - Additional columns show counts for the computers and contacts selected and available in each OU/container.
2. Select an OU/container that shows a count for one or more computers.

> **Note:** Sort this tab by clicking the **Sort Descending** option in the **Total Computers** column heading. This ensures any OU/containers with computer counts greater than zero are listed first.

3. Select the **Computers Policy** button.
   - The dialog box lists all the available computers of the OU/container you can *include* *(page 35)* in selected policies.
   - Entering a checkbox next to a computer in this dialog means you want to install an agent on that domain computer.
   - ✓ If the **Automatically install Agents when computer is discovered** checkbox in the **Agent Deployment Policy** *(page 27)* tab is checked, then agents will be installed automatically to selected computers of this OU/container as soon as the domain computers are rebooted. If this same

checkbox is not checked, you must deploy agents manually by selecting the **machine ID template** *(page 36)* account created for a domain computer in the **Computers** *(page 18)* page, then clicking the **Deploy Agent** button on the same page. The domain computer must still be rebooted to complete the agent installation.

- Optionally checking the **Automatically assign portal access to portal candidates** means you also want to designate these computers as **portal candidate machines** *(page 8)*.
- Optionally checking the **Include new Computers** checkbox means you want to *include* new computers added to this OU/container. They will be assigned the same KDS policy you have previously configured for selected computers in this OU/container.

4. Check one or more computers in the list and click **Save**.
   - The dialog closes and the count in the **Selected Computers** column is updated with the number of machines included in the computer policy you just set.
   - The **Probe Status** displays `Activated` and the **Computers/Contacts Status** displays `Modified` because the policy changes just made have not yet been applied.

> **Note:** The **Apply Changes** button should only be clicked when policies for both the **Computer / Contact Policies** *(page 28)* and **User Policies** *(page 29)* tabs are *completed*. The **Apply Changes** button applies changes made to both tabs.

Configuring Contact Policies

1. Click the Directory Services > Domains > **Computer / Contact Policies** *(page 28)* tab.
   - Use this tab to specify which domain contacts you want to create a staff record for in the VSA. A domain **contact** contains contact information similar to information defined for a user, but a contact has no domain logon privileges.
   - Each OU/container in this tab is identified by its canonical name. A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
   - Additional columns show counts for the computers and contacts selected and available in each OU/container.
2. Select a OU/container that shows a count for one or more contacts.

   > **Note:** Sort this tab by clicking the **Sort Descending** option in the **Total Contacts** column heading. This ensures any OU/containers with contact counts greater than zero are listed first.

3. Select the **Contacts Policy** button.
   - The dialog box lists all the available contacts of the OU/container you can *include* *(page 35)* in selected policies.
   - Entering a checkbox next to a contact in this dialog means you want to create a VSA staff record for that domain contact.
   - Optionally checking the **Include new Contacts** checkbox means you want to *include* new contacts added to this OU/container. VSA staff records will be created for these new contacts as they are discovered.
4. Check one or more contacts in the list and click **Save**.
   - The dialog closes and the count in the **Selected Contacts** column is updated with the number of contacts included in the contact policy you just set.
   - The **Probe Status** displays `Activated` and the **Computers/Contacts Status** displays `Modified` because the policy changes just made have not yet been applied.

> **Note:** The **Apply Changes** button should only be clicked when policies for both the **Computer / Contact Policies** *(page 28)* and **User Policies** *(page 29)* tabs are *completed*. The **Apply Changes** button applies changes made to both tabs.

Configuring User Policies

1. Click the Directory Services > Domains > **Users** *(page 29)* tab.
   - ➢ KDS user policies enable users to logon to the VSA or to **Portal Access** *(page 8)* using their domain credentials.
   - ➢ Each domain credential can be applied to *only one* of two kinds of VSA logons:
   - ✓ **VSA user logons** - These logons are used by VSA administrators.
   - ✓ **Portal Access logons** - These logons are used by machine users who want to access their own machines remotely.
   - ➢ User groups are simply called "groups" in an Active Directory domain. Each group in this tab is identified by its canonical name. A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
   - ➢ An additional column shows a count for the number of users in each group.
2. Select a group that shows a count for one or more users.
   - ➢ The same member can be a member of multiple groups in an Active Directory domain.

   > **Note:** Sort this tab by clicking the **Sort Descending** option in the **Users Policies** column heading. This ensures any groups with user counts greater than zero that don't yet have policies assigned are listed near the top of the tab.

3. Select the **Configure Users Policy** button.
   - ➢ The **Users Policy** dialog displays, listing the **Member Users** in this group.
4. Select a **Member Group Policy.**
   - ➢ Each user group in KDS can be assigned one of three different VSA logon policies. These policies are applied to all users belonging to the group. They cannot be applied to individual users within a group.
   - ✓ `Do Not Include Users` - Do not create VSA user logons or Portal Access logons for domain users listed in this user group.
   - ✓ `Create Staff Members` - Creates a staff member record. These users can be assigned Portal Access to a machine *manually*.
   - ✓ `Create Staff and make Auto Portal Candidates` - Designates domain users in this user group as Portal Access candidates. See **Making Portal Access Candidates** *(page 8)* for details.
   - ✓ `Create VSA Users` - Creates VSA user logons for domain users listed in this user group.
   - ➢ *Since each domain user can belong to multiple domain user groups, a domain user is assigned the* **highest ranking VSA logon policy** *assigned to any user group the domain user is a member of.*
   - ✓ `Create VSA Users` outranks `Create Staff and make Auto Portal Candidates`
   - ✓ `Create Staff and make Auto Portal Candidates` outranks `Create Staff Members`
   - ✓ `Create Staff Members` outranks `Do Not Include Users`
5. If `Create VSA Users` is selected:
   - ➢ **Role Lookup** - Select the role these users will use.
   - ➢ **Scope Lookup** - Select the scope these users will use.

- If *a scope with the same name as the organization* does not already exist, a + displays to the right of the **Scope Lookup** drop-down list of the **User Policy** dialog. Clicking the + icon enables you to create a new scope that has the same name as the organization associated with the domain. Once the scope is created the + no longer displays to the right of the **Scope Lookup** drop-down list and text at the top of the dialog indicates the default scope already exists.
- If the same user is assigned to multiple groups, and different roles and scopes are assigned to each group, then when the user logs on to the VSA, these roles and scopes will be available in the roles/scope selector in the upper-right corner of the VSA window.

> **Note:** Roles/scope assignments using **User Policies** can be modified and reapplied multiple times. Successive changes will cause roles and scopes to *accumulate, rather than be replaced*. KDS never removes records in the VSA.

6. Click **Save** to close this dialog.
   - The dialog closes and the policy you selected displays in the **Users Policy** column.
7. If you've already configured KDS policies for computers and contacts, click the **Apply Changes** button.

> **Note:** The **Apply Changes** button should only be clicked when policies for both the **Computer / Contact Policies** *(page 28)* and **User Policies** *(page 29)* tabs are *completed*. The **Apply Changes** button applies changes made to both tabs.

8. Now that policies are applied, return to the **Agent Deployment Policy** *(page 14)* tab and check the **Automatically install Agents when computer is discovered**, if this checkbox is not already checked.

Configuring Alert Policies

1. Click the Directory Services > Domains > **Alert Policies** *(page 31)* tab.
2. Enable all probe alerts.

> **Warning:** The KDS probe accumulates domain *changes* in real time. If the connection between the KDS probe and a domain is lost for a period of time, the probe has no way to recover those changes. To ensure domain changes are not lost forever, set **probe alerts** *(page 12)* and schedule a recurring *full* **synchronization** *(page 10)*. *If a probe alert is triggered, consider running a full synchronization immediately.*

3. Enable selected domain alerts.
   - If agents are deployed automatically using the **Automatically install Agents when computer is discovered** checkbox in **Agent Deployment Policy** *(page 27)*, you do not need to be notified about the discovery of new computers. If agents are not installed automatically, *you do need to be notified* about newly discovered computers.
   - Enable alarms and email notification for the creation, and deletion of organizational units, containers and groups. You may need to review KDS policies after creating or deleting one of these folder objects. KDS computer and contact policies are set using organization units and containers. KDS user policies are set using groups.

Configuring Schedule and Status

1. Click the Directory Services > Domains > **Schedule and Status** *(page 32)* tab.
2. Enable full synchronization on a weekly basis.

> **Warning:** The KDS probe accumulates domain *changes* in real time. If the connection between the KDS probe and a domain is lost for a period of time, the probe has no way to recover those changes. To ensure domain changes are not lost forever, set **probe alerts** *(page 12)* and schedule a recurring *full*

> **synchronization** *(page 10)*. *If a probe alert is triggered, consider running a full synchronization immediately.*

Computers

Directory Services > Computers

The **Computers** page lists **machine ID / group ID /organization ID** *(page 36)* accounts created, based on applied KDS computer policies, for all domains monitored by KDS probes.

Newly created machine ID accounts initially display as "empty" machine ID template accounts—identified with a ▣ check-in icon—meaning there is no corresponding agent for this machine ID account.

Changes made to **included** *(page 35)* computers update their corresponding VSA machine ID accounts at the next synchronization.

For more information see:

- **How Agents are Installed Using KDS** *(page 6)*
- **How Machine ID Accounts are Created in KDS** *(page 7)*
- **How Machine Moves in Domains are Reflected in KDS** *(page 7)*

Upper Pane

Actions

- **Deploy Agent** - If an agent has not yet been deployed for a created machine ID account, you can manually deploy the agent using this page.
- **Merge Duplicates** - If a duplicate machine ID accounts for the same domain computer. If an agent already exists on a managed machine in a different machine group, then KDS creates an "empty" **machine ID template** *(page 36)* account—identified with a ▣ check-in icon—and no agent ever checks in. The new machine ID template account displays a **machine.ID / group ID / organization ID** *(page 36)* based on the computer's canonical name in the Active Directory domain. *You can merge these duplicate accounts.* The existing, active agent account adopts the name of the new machine ID template account, then the new machine ID template account is deleted. No data is lost by the merge and the machine ID account now matches its location in the domain hierarchy.

Column Headings

- **Machine.Group ID** - A unique **machine ID / group ID / organization ID** *(page 36)* name for a machine in the VSA.
- **Domain Name** - The name of the Active Directory domain.
- **Duplicate Exists** - If checked, a duplicate VSA machine ID account exists for this domain computer.
- **Duplicate Machine Group ID** - The name of a duplicate machine.group ID for this same machine.
- **Agent Deployed** - If checked, an agent has been deployed on this computer.
- **Install Package** - The agent install package selected for this computer's domain.
- **OS** - The operating system of the computer.
- **Auto Portal** - A domain user is automatically assigned to be the **Portal Access** *(page 8)* user of domain machine if **Auto Portal** is enabled for *both* the domain user and domain computer.
- **Canonical Name** - A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.

Lower Pane

The lower pane displays detailed information about a row selected in the upper pane.

VSA Agent Settings

- **Machine ID** - A unique **machine ID / group ID / organization ID** *(page 36)* name for a machine in the VSA.
- **Agent Deployment Package** - The agent install package selected for this computer's domain.

Status

- **Operating System** - The operating system of the computer.
- **Last Reboot** - The last date/time the computer was rebooted.
- **Created in AD** - The date/time the computer was added to the Active Directory domain.
- **Last Modified in AD** - The date/time the computer record in the Active Directory domain was last modified.
- **Last Logged-on User ID** - The user ID of the last logon to the computer.
- **Last Logged-on User Name** - The user name of the last logon to the computer.

Directory Server Details

Describes detailed information about the computer in the domain.

- **Computer Name** - The name of the computer.
- **Domain Name** - The name of the Active Directory domain.
- **Canonical Name** - A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
- **Distinguished Name** - A **distinguished name** provides the same information as a canonical name, formatted as a series of attributes, sequenced in reverse order from the canonical name. CN = Common name or container. OU = Organization unit. DC = Domain component.
- **DNS Host Name** - The fully qualified domain name of the computer.
- **DC Type** - `Domain Server` or `Domain Member`.
- **Site** - The name of a geographical location, comprising one or more subnets. A local area network (LAN).
- **Description** - A one line description of the computer.
- **Location** - The site/subnet of the computer. Used to locate nearby printers and other resources.
- **Primary Group** - A user or computer is associated with a **primary group** for POSIX compliance, based on UNIX. For Active Directory domain computers, the default primary group is `Domain Computers`.

Contacts

Directory Services > Contacts

The **Contacts** page lists staff records created, based on applied KDS contact policies, for all domains monitored by KDS probes.

Changes made to **included** *(page 35)* domain contacts update their corresponding VSA staff records at the next synchronization.

Upper Pane

Note: There are no actions you can take on this page.

Column Headings

- **Contact** - The canonical name for the domain contact. A A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
- **Staff** - The full name of the staff record created in the VSA.
- **VSA Org** - The VSA organization of the staff record.
- **VSA Dept** - The VSA department of the staff record.
- **Email** - The email of the staff record.
- **Telephone No** - The phone number of the staff record.
- **Mobile** - The mobile phone number of the staff record.

Lower Pane

The lower pane displays detailed information harvested from the domain about a contact selected in the upper pane.

General

- **First Name** - The first name of the contact.
- **Last Name** - The last name of the contact.
- **Display Name** - The full name of the contact.
- **Description** - A description of the contact.
- **Office** - The contact's office location.
- **Telephone Numbe**r - The primary phone number of the contact.
- **Email** - The email of the contact.

Address

The address of the contact.

- **Street**
- **P.O. Box**
- **City** -
- **State/Province**
- **Zip/Postal Code**
- **Country/Region**

Telephones

The phones numbers and notes for the contact.

- **Home**
- **Pager**
- **Mobile**
- **Fax**
- **IP Phone**
- **Notes**

Account

- **Common Name** - The common name of the contact.
- **Canonical Name** - The canonical name of the contact. A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
- **Domain Name** - The name of the Active Directory domain.

- **Distinguished Name** - A **distinguished name** provides the same information as a canonical name, formatted as a series of attributes, sequenced in reverse order from the canonical name. CN = Common name or container. OU = Organization unit. DC = Domain component.
- **Description** - A description of the contact.
- **Created in AD** - The date/time the contact record was created in the Active Directory domain.
- **Last Modified in AD** - The date/time the contact record was last modified in the Active Directory domain.

Organization

- **Job Title** - The job title of the contact.
- **Department** - The department the contact is a member of.
- **Company** - The company the contact is a member of.
- **Manager** - The manager of this contact.
- **Direct Reports** - The users or contacts that report to this contact.

Users and Portal Users

Directory Services > Users and Portal Access

The **Users and Portal Access** lists VSA users and Portal Access candidates created, based on applied KDS group policies, for all domains monitored by KDS probes.

Changes made **included** *(page 35)* domain (user) groups update their corresponding VSA user and Portal Access candidate records at the next synchronization.

For more information see:

- **Setting KDS Policies for Users** *(page 5)*
- **Enabling Portal Access in KDS** *(page 8)*
- **Enabling/Disabling Domain Users Accounts or Resetting Domain User Password** *(page 9)*
- **Making Changes to KDS Managed User Logons** *(page 9)*

Upper Pane

Actions

- **Disable Account** - Disables a domain user account immediately. Affects VSA logons and Portal Access logons using the same domain logon.
- **Enable Account** - Enables a domain user account immediately. Affects VSA logons and Portal Access logons using the same domain logon.
- **Reset Password** - Resets a domain user password. The effect takes effect at the next logon. Affects VSA logons and Portal Access logons using the same domain logon.
- **Assign Portal User** - Manually assigns Portal Access to a domain computer *to* a domain user.
- **Remove Portal Users** - Manually removes Portal Access to a domain computer *from* a domain user.
- **Refresh** - Refreshes the page.

Column Headings

- **Domain Name** - The name of the Active Directory domain.
- **Domain User** - The fully qualified domain name of the user.
- **User Name** - The domain user name.
- **User Login Name** - The VSA logon name, if this is also a VSA user logon.
- **Enabled** - If checked, the user is enabled in the domain.
- **VSA Org** - The VSA **organization** *(page 37)* this user is a member of.

- **VSA Dept** - The VSA department this user is a member of.
- **Supervisor** - The VSA supervisor for this staff member.
- **Expires** - The date this account expires.
- **VSA** - If checked, the VSA user can logon to the VSA using his or her domain credential.
- **Portal** - If checked, this domain user is assigned the Portal Access user of the domain machine listed in the **Portal Assignment** column. Unchecked, the user is not assigned to any domain computer as the Portal Access user.
- **Auto Portal** - A domain user is automatically assigned to be the **Portal Access** *(page 8)* user of a domain machine if **Auto Portal** is enabled for *both* the domain user and domain computer.
- **Portal Assignment**
  - `None (will be assigned upon login to an 'Auto Portal' computer)` - Auto Portal is enabled for this user.
  - `None (assign using the 'Assign Portal User' button)` - Auto Portal is not enabled for this user, but can be manually assigned to be the Portal Access user of a machine.
  - `<machineID>` - The domain computer currently assigned to the domain user with Portal Access to that machine.
  - `VSA User` - The user is a VSA user and cannot be assigned as a Portal Access user of a machine.
- **Last Logged-on to (Machines)** - The domain computer the domain user last logged on to. Portal Access to a domain machine can only be assigned to the last machine a domain user has logged on to.
- **Email** - The email of the domain user.
- **Phone** - The phone of the domain user.
- **City** - The city of the domain user.
- **Country** - The country of the domain user.
- **User Policy** - The policy assigned to the user.

Lower Pane

The lower pane displays detailed information harvested from the domain about a user selected in the upper pane.

User Details

General

- **First Name** - The first name of the user.
- **Last Name** - The last name of the user.
- **Display Name** - The full name of the user.
- **Office** - The user's office location.
- **Telephone Number** - The primary phone number of the user.
- **Email** - The email of the user.
- **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.
- **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.
- **Timesheet 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.

- **VSA Logon** - If `Yes`, the VSA can logon to the VSA using his or her domain credential.
- **VSA Roles** - The VSA roles assigned to the VSA user.
- **VSA Scopes** - The VSA scopes assigned to the VSA user.

Address

The address of the user.

- **Street**
- **P.O. Box**
- **City**
- **State/Province**
- **Zip/Postal Code**
- **Country/Region**

Telephones

The phones numbers and notes for the user.

- **Home**
- **Pager**
- **Mobile**
- **Fax**
- **IP Phone**
- **Notes**

Account

- **User Logon Name** - The domain user's logon name.
- **Account Expires** - The expiration date for the domain account.
- **Common Name** - The common name of the user in the domain.
- **Canonical Name** - The canonical name of the user. A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
- **Domain Name** - The name of the Active Directory domain.
- **Distinguished Name** - A **distinguished name** provides the same information as a canonical name, formatted as a series of attributes, sequenced in reverse order from the canonical name. CN = Common name or container. OU = Organization unit. DC = Domain component.
- **Last Password Change** - The last date the password changed.
- **Last Logon** - The date/time the user last logged on.
- **Last Logoff** - The date/time the user last logged off.
- **Created in AD** - The date/time the user record was created in the Active Directory domain.
- **Last Modified in AD** - The date/time the user record was last modified in the Active Directory domain.

Organization

- **Title** - The job title of the user.
- **Domain Department** - The department the user is a member of.
- **VSA Department** - The department the VSA staff record is a member of.
- **Domain Company** - The company the user is a member of.
- **Supervisor** - The user or contact this user reports to. Called the `Manager` in domain and `Supervisor` in VSA.
- **VSA Org Id** - The VSA identifier of the **organization** *(page 37)*.
- **VSA Org Name** - The VSA friendly name of the organization.

- **Description** - A description of the domain user account.
- **Direct Reports** - The domain contacts or domain users that report to this domain user.

Portal Access tab

Additional details display in the **Portal Access** tab if the user is a **Portal Access candidate** *(page 8)*.

VSA Portal Settings

These settings are the same as those shown on the Agent > Portal Access page.

- **Portal Access Enabled** - If `Yes`, the domain user is currently assigned a Portal Access remote logon to a VSA managed machine.
- **User ID** - The Portal Access user ID.
- **Contact Name** - The name for the Portal Access user.
- **Contact Email** - The name for the Portal Access user.
- **Contact Phone** - The phone for the Portal Access user.

> **Note:** The **Change Profile** tab of Portal Access is automatically populated with the *name*, *email* and *phone number* of the currently logged in Portal Access candidate. The submitter fields of new **Service Desk** tickets are populated with the contact information stored in the **Change Profile** tab. This means Portal Access users don't have re-enter the same contact information, each time they create a new **Service Desk** ticket.

- **Language Preference** - The Portal Users language preference.
- **Machine Role** - The machine role assigned to the Portal Access machine.
- **Show Notes as Tooltip** - If checked, Agent > 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.
- **Auto Assign Tickets from inbound emails** - If `Yes`, auto assign a ticket to this machine ID if the Ticketing email reader 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.

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

- **Portal Assignment** - The machine the Portal Access user is assigned to.
- **Last Logged-on to Machine** - The date/time the Portal Access user last logged onto the machine.

VSA Machine Administrator

- **Admin Email** - The email address providing administrator support for this managed machine. Set using the Agent > Edit Profile page.

Computer Manager from Directory Server

- **Manager** - The domain user this domain user reports to. Called the `Manager` in an Active Directory domain and `Supervisor` in the VSA.
- **Office** - The user's office location.
- The user's address:
  - **Street**
  - **City**
  - **State/Province**
  - **Country/Region**
- **Telephone No.** - The user's phone number.
- **Fax No.** - The user's fax number.

Domains

Directory Services > Domains

The **Domains** page configures the integration of KDS with Active Directory domains. Configuration features include:

- Installing KDS probes that monitor a domain.
- Activating and scheduling the synchronization of data between KDS and the domain.
- Applying KDS policies for:
  - The deployment of agents.
  - The creation of VSA users, Portal Access users and staff records.
- Setting KDS alerts.
- Displaying the status of the KDS configuration.

Information about a domain selected in the upper pane of the **Domains** page is organized into the following tabs in the lower pane. *Configure a selected domain in the tab order presented, from left to right.*

1. **Probe Deployment** *(page 26)*
2. **Agent Deploy Policy** *(page 27)*
3. **Computer / Contact Policies** *(page 28)*
4. **User Policies** *(page 29)*
5. **Alert Policies** *(page 31)*
6. **Schedule and Status** *(page 32)*

Upper Pane

Actions

- **Refresh** - Refreshes the entire page.

Column Headings

- **Domain Name** - The name of the Active Directory domain.
- Domain Guid -
- **Org Id** - The VSA identifier of the **organization** *(page 37)*.
- **Org Name** - The VSA friendly name of the organization.
- **Probe Status**

  ⊖ - Un-installed - A probe is not installed for this domain.

  ◉ - Processing - The probe executing a user request.

  ◎ - Installed - The probe is installed and harvesting has been completed.

  ✅ - Activated - The probe is monitoring the domain. KDS policies are not modified.

  ✔ - Activated - The probe is monitoring the domain. KDS policies are modified but have not yet been applied.

  ✔ - Activated - The probe is monitoring the domain. KDS policies have been modified but not yet been applied for at least three synchronization intervals. The KDS administrator may have forgotten to apply the modified policies.

  ❗ - Attention - The probe has encountered a problem that may require user attention. Because the probe's attention status may self-correct, the attention status does not necessarily correspond to a warning alert or error alert.

  Note: KDS pages are not auto-refreshed. Click the **Refresh** button to ensure the latest Probe Status displays.

- **Computers/Contacts** / **User Policies Status** - The policies of both tabs can be in one of 3 states.
  - Original - KDS policies have not yet been configured.
  - Modified - KDS policies have been configured but not yet applied. After clicking the **Apply Changes** button, this icon remains unchanged until the harvest has been completed.
  - ✓ - Applied - KDS policies have been applied.
- **Last Probe Agent Check-in** - The latest date/time the probe agent checked in.
- **Last Probe Response** -
- **Last Status Message** -

Probe Deployment

Directory Services > Domains > Probe Deployment tab

The **Probe Deployment** tab configures the probe agent for a selected domain. All domain computers with a Kaseya agent installed on them display in the lower panel.

KDS communicates with an Active Directory domain using a **probe agent**. The probe uses the industry standard LDAP protocol to safely and securely communicate with domain. Each probe agent must be a member of the domain it monitors. Probe deployment installs the extra functionality an agent requires to act as a probe.

Initially you may only see a single domain computer with a Kaseya agent installed on it displayed in the lower pane. As agents are automatically installed on other domain computers using KDS policies, these domain computers will all be displayed in the lower pane.

For more information see:

- **Configuring Probe Deployment** *(page 13)*.

Lower Pane

Header Fields

- **Probe Status**
  - ⊖ - Un-installed - A probe is not installed for this domain.
  - ◉ - Processing - The probe executing a user request.
  - ◎ - Installed - The probe is installed and harvesting has been completed.
  - ✓ - Activated - The probe is monitoring the domain. KDS policies are not modified.
  - ✓ - Activated - The probe is monitoring the domain. KDS policies are modified but have not yet been applied.
  - ✓ - Activated - The probe is monitoring the domain. KDS policies have been modified but not yet been applied for at least three synchronization intervals. The KDS administrator may have forgotten to apply the modified policies.
  - ❗ - Attention - The probe has encountered a problem that may require user attention. Because the probe's attention status may self-correct, the attention status does not necessarily correspond to a warning alert or error alert.

  > **Note:** KDS pages are not auto-refreshed. Click the **Refresh** button to ensure the latest Probe Status displays.

- **Domain Name** - The name of the Active Directory domain.
- **Administrator User Name** - The administrator name of the credential used to log into the Active Directory domain.

Actions

- **Install** - Installs the probe.
- **Uninstall** - Uninstalls the probe.

> **Note:** Before uninstalling the KDS module from the VSA be sure to deactivate and detach the organization, then uninstall the probe agent.

- **Activate** - Activates the probe.
- **Deactivate** - Deactivates the probe.
- **Deactivate and Detach Org** - Deactives the probe and detaches the organization. This may be necessary if the wrong organization was selected for the domain initially. See **Deactivation** *(page 11)* for issues to consider before *deactivating* a probe.
- **Refresh** - Refreshes the lower pane.

Column Headings

- **Domain Name** - The name of the Active Directory domain.
- **Machine.Group ID** - The machine ID.groupID.orgID of the machine in the VSA.
- **dns Computer Name** - The fully qualified domain name of the computer.
- **Computer Name** - The local host name of the computer.
- **Agent Guid** - A unique identifier for a machine ID.group ID account and its corresponding agent.
- **ip Address** - The IP address of the computer.
- **Domain Guid** - The unique GUID identifying this domain in KDS.
- **Host Type** - `Domain Server` or `Domain Member`.
- **Status** - The probe status of the machine.
- **Last Agent Check-in** - The last time the agent for this machine is checked in.
- **Organization** - The VSA **organization** *(page 37)* this computer is a member of.

Agent Deployment Policy

Directory Services > Domains > Agent Deployment Policy tab

The **Agent Deployment** tab sets agent deployment policies for a selected domain.

For more information see:

- **Configuring Agent Deployment Policy** *(page 14)*.

Header Fields

- **Probe Status**

  ⊖ - Un-installed - A probe is not installed for this domain.

  ◉ - Processing - The probe executing a user request.

  ◎ - Installed - The probe is installed and harvesting has been completed.

  ✅ - Activated - The probe is monitoring the domain. KDS policies are not modified.

  ✔ - Activated - The probe is monitoring the domain. KDS policies are modified but have not yet been applied.

  ✔ - Activated - The probe is monitoring the domain. KDS policies have been modified but not yet been applied for at least three synchronization intervals. The KDS administrator may have forgotten to apply the modified policies.

  ❗ - Attention - The probe has encountered a problem that may require user attention. Because the probe's attention status may self-correct, the attention status does not necessarily correspond to a warning alert or error alert.

> **Note:** KDS pages are not auto-refreshed. Click the **Refresh** button to ensure the latest Probe Status displays.

Actions

- **Edit** - Edit agent deployment policies.
  - **Automatically install Agents when computer is discovered** - Check this checkbox. When policies are applied, agents are automatically installed on computers that are members of those policies. *The computers must be rebooted to complete the installation of the Kaseya agents.*
  - **Allow Agents to be installed on Directory Server** - Leave this checkbox blank. If checked, agents will also be installed on the system hosting the Active Directory domain.
  - **Default Package** - Select the agent install package to use with the selected domain. See **How Agents are Installed Using KDS** *(page 6)*

Computer / Contact Policies

Directory Services > Domains > Computer / Contact Policies tab

The **Computer / Contact Policies** tab sets KDS policies for computers and contacts for a selected domain.

Once a probe is installed, KDS is configured by setting selected domain folders and items to **included** or **excluded**. KDS policies provide IT automation—such as installing agents or creating users—only for *included* folders and items. KDS only harvests detailed information for *included* folders and items, minimizing the amount of data required to maintain synchronization with the domain.

For more information see:

- **Setting KDS Policies for Computers** *(page 5)*
- **Setting KDS Policies for Contacts** *(page 5)*
- **Configuring Computer Policies** *(page 14)*
- **Configuring Contact Policies** *(page 15)*.

Header Fields

- **Computer / Contacts Status**

  - Original - KDS policies have not yet been configured.

  - Modified - KDS policies have been configured but not yet applied. After clicking the **Apply Changes** button, this icon remains unchanged until the harvest has been completed.

  - Applied - KDS policies have been applied.
- **Last Full Sync** - Date/time of last full synchronization for this domain.
- **Last Incremental Sync** - Date/time of last incremental synchronization of all outstanding changes for this domain.

Actions

- **Computers Policy** - Sets the KDS computer policy for included computers in an OU/container.
  - Include new Computers
  - Automatically assign portal access to portal candidates
- **Contacts Policy** - Sets the KDS contact policy for included contacts in an OU/container.
  - Include new Contacts
- **Apply Changes** - Applies KDS policies set on both the Computer / Contact Policies tab and the User Policies tab.

Column Headings

- **Type**

  - Domain

  - Container

  - Organizational Unit
- **Container/Org Unit** - The canonical name of a container or organizational unit in the Active Directory domain. A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
- **Include New Computers** - If checked, newly discovered machines are included.
- **Selected Computers** - Represents the number of machines that have are *included* in this OU/container. Initially this number is zero.-
- **Total Computers** - Represents the total number of machines that are members of this OU/container.
- **Auto Portal Computers** -
- **Incl New Contacts** -
- **Selected Contacts** - represents the number of contacts that are *included* in this OU/container. Initially this number is zero.
- **Total Contacts** - represents the total number of contacts that are members of this OU/container.

User Policies

Directory Services > Domains > User Policies tab

The **Groups / Users Policies** tab sets KDS policies for (user) groups for a selected domain.

Once a probe is installed, KDS is configured by setting selected domain folders and items to **included** or **excluded**. KDS policies provide IT automation—such as installing agents or creating users—only for *included* folders and items. KDS only harvests detailed information for *included* folders and items, minimizing the amount of data required to maintain synchronization with the domain.

For more information see:

- **Setting KDS Policies for Users** *(page 5)*
- **Configuring User Policies** *(page 16)*
- **Managing Remote Portal Access** *(page 4)*
- **Enabling Portal Access in KDS** *(page 8)*
- **Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords** *(page 9)*
- **Making Changes to KDS Managed User Logons** *(page 9)*

Header Fields

- **User Policies Status**

  - Original - KDS policies have not yet been configured.

  - Modified - KDS policies have been configured but not yet applied. After clicking the **Apply Changes** button, this icon remains unchanged until the harvest has been completed.

  - Applied - KDS policies have been applied.
- **Last Full Sync** - Date/time of last full synchronization for this domain.
- **Last Incremental Sync** - Date/time of last incremental synchronization of all outstanding changes for this domain.

Actions

- **Do not include Users** - *Excludes* all users in a selected group.
- **Configure Users Policy** - *Includes* selected users as either VSA users *or* Portal Access candidates.

  - ➢ `Do Not Include Users` - Do not create VSA user logons or Portal Access logons for domain users listed in this user group.
  - ➢ `Create Staff Members` - Creates a staff member record. These users can be assigned Portal Access to a machine *manually*.
  - ➢ `Create Staff and make Auto Portal Candidates` - Designates domain users in this user group as Portal Access candidates. See **Making Portal Access Candidates** *(page 8)* for details.
  - ➢ `Create VSA Users` - Creates VSA user logons for domain users listed in this user group.
  - ✓ Role Lookup
  - ✓ Scope Lookup
  - ➢ If *a scope with the same name as the organization* does not already exist, a + displays to the right of the **Scope Lookup** drop-down list of the **User Policy** dialog. Clicking the + icon enables you to create a new scope that has the same name as the organization associated with the domain. Once the scope is created the + no longer displays to the right of the **Scope Lookup** drop-down list and text at the top of the dialog indicates the default scope already exists.
  - ➢ If the same user is assigned to multiple groups, and different roles and scopes are assigned to each group, then when the user logs on to the VSA, these roles and scopes will be available in the roles/scope selector in the upper-right corner of the VSA window.

    > **Note:** Roles/scope assignments using **User Policies** can be modified and reapplied multiple times. Successive changes will cause roles and scopes to *accumulate, rather than be replaced*. KDS never removes records in the VSA.

- **Apply Changes** - Applies KDS policies changes for both the **Computer / Contact Policies** tab and the **User Policies** tab.

  > **Note:** Do not **Apply Changes** until policies are set on both tabs.

- **Refresh** - Refreshes this tab.

Column Headings

- **Type** -
- **Group Name** - A **canonical name** provides the *complete hierarchy of OUs/containers* used to locate folders and items—such as computers, contacts or groups—in a domain, similar in format to the full path name of a file in a disk directory.
- **Users Policy**
  - ➢ `Do Not Include Users` - Do not create VSA user logons or Portal Access logons for domain users listed in this user group.
  - ➢ `Create Staff Members` -
  - ➢ `Create Staff and make Auto Portal Candidates` - Designates domain users in this user group as Portal Access candidates. See **Making Portal Access Candidates** *(page 8)* for details.
  - ➢ `Create VSA Users` - Creates VSA user logons for domain users listed in this user group.
- **Role Policy** - The VSA role to assign to newly created VSA users if **Users Policy** is `Create VSA Users`. Role policy can also be set to.
  - ➢ `Use existing Role`
  - ➢ `Do not create Role`
- **Scope Policy** - The VSA scope to assign to newly created VSA users if **Users Policy** is `Create VSA Users`. Scope policy can also be set to.
  - ➢ `Use existing Scope`

- Do not create Scope

Alert Policies

Directory Services > Domains > Alert Policies tab

The **Alerts Policies** tab sets KDS alert policies for a selected domain.

For more information see:

- **Probe Alerts and Domain Alerts** *(page 12)*
- **Configuring Alert Policies** *(page 17)*

Actions

- **Configure** - Edits probe and domain alert policy settings displayed on this tab.

Probe Alerts Policy

Displays enabled/disabled *probe* alert policy settings.

- Alarm on Warning
- Ticket on Warning
- Email on Warning
- Email Addresses (for warning)
- Alarm on Failure
- Ticket on Failure
- Email on Failure
- Email Addresses (for failure)

Domain Alerts Policy

Displays enabled/disabled *domain* alert policy settings.

- Type / Object Type
  - - Computer
  - - Contact
  - - Container
  - - Domain
  - - Group
  - - Organizational Unit
  - - User
- Alarm on create
- Alarm on change
- Alarm on delete
- Ticket on create
- Ticket on change
- Ticket on delete
- Email on create
- Email on change
- Email on delete
- Email Addresses

Schedule and Status

Directory Services > Domains > Schedule and Status tab

The **Schedule and Status** tab schedules full synchronizations for a selected domain. It also displays the status of the incremental synchronization and full synchronizations.

For more information see:

- **Synchronization** *(page 10)*

Actions

- **Schedule Full Synchronization** - Schedules a full synchronization once or periodically. Each type of recurrence—Once, Minutes, 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. 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 Full Synchronization** - Cancels the full synchronization schedule.

Header Fields

- **Probe Status**

  ⊜ - Un-installed - A probe is not installed for this domain.

  ◉ - Processing - The probe executing a user request.

  ○ - Installed - The probe is installed and harvesting has been completed.

  ✓ - Activated - The probe is monitoring the domain. KDS policies are not modified.

  ✓ - Activated - The probe is monitoring the domain. KDS policies are modified but have not yet been applied.

  ✓ - Activated - The probe is monitoring the domain. KDS policies have been modified but not yet been applied for at least three synchronization intervals. The KDS administrator may have forgotten to apply the modified policies.

  ❗ - Attention - The probe has encountered a problem that may require user attention. Because the probe's attention status may self-correct, the attention status does not necessarily correspond to a warning alert or error alert.

  > **Note:** KDS pages are not auto-refreshed. Click the **Refresh** button to ensure the latest Probe Status displays.

- **Computers/Contacts Status** and **User Policies Status**

  ▣ - Original - KDS policies have not yet been configured.

  ▣ - Modified - KDS policies have been configured but not yet applied. After clicking the **Apply Changes** button, this icon remains unchanged until the harvest has been completed.

  ▣ - Applied - KDS policies have been applied.

General Information

- **Domain Name** - The name of the Active Directory domain.

- **Incr. Sync. Interval (mins)** - The incremental synchronization interval for this domain. The synchronization interval is set when a probe is activated using the **Probe Deployment** *(page 26)* tab.
- **Administrator User Name** - The administrator name of the credential used to log into the Active Directory domain.

Synchronization History

- **Recent Agent Check-in** - The most recent check-in of any agent on the domain.
- **Active Agent Check-in** - Date/time the probe agent of this domain last checked in.
- **Last Probe Request** - Date/time a synchronization request was last sent to the probe of this domain.
- **Last Script Exec.** - Date/time a script was last executed for this domain.
- **Last Full Preview** - Date/time a preview synchronization was last executed for this domain. A preview is only performed when a probe is installed.
- **Last Full Sync** - Date/time of last full synchronization for this domain.
- **Last Incremental Sync** - Date/time of last incremental synchronization of all outstanding changes for this domain.
- **Last Script Status** - Status of last KDS script executed for this domain. For example, `Then/Else Success` or `Then/Else failure in step N`.

Scheduled Synchronization

- **Full Synchronization Period** - The scheduled pattern for full synchronization for this domain. May be once or recurring.
- **Next Full Synchronization** - The next scheduled full synchronization for this domain.

Audit Log

Directory Services > Audit Log

The **Audit Log** page displays a log of **Directory Services** module activity by:

- **Event ID**
- **Event Date**
- **Admin**
- **Event Name**
- **Message**

If information has changed or been removed unexpectedly, check this page to determine what events and administrators may have been involved.

This table supports selectable columns, column sorting, column filtering and flexible columns widths.

Glossary of Terms

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** *(page 36)*. 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.

Contact

A domain **contact** contains contact information similar to information defined for a user, but a contact has no domain logon privileges.

Distinguished Name

A **distinguished name** provides the same information as a canonical name, formatted as a series of attributes, sequenced in reverse order from the canonical name. CN = Common name or container. OU = Organization unit. DC = Domain component.

Duplicate Exists

If an agent already exists on a managed machine in a different machine group, then KDS creates an "empty" **machine ID template** *(page 36)* account—identified with a check-in icon—and no agent ever checks in. The new machine ID template account displays a **machine.ID / group ID / organization ID** *(page 36)* based on the computer's canonical name in the Active Directory domain. *You can merge these duplicate accounts.* The existing, active agent account adopts the name of the new machine ID template account, then the new machine ID template account is deleted. No data is lost by the merge and the machine ID account now matches its location in the domain hierarchy.

Included / Excluded domain Folders and Items

Once a probe is installed, KDS is configured by setting selected domain folders and items to **included** or **excluded**. KDS policies provide IT automation—such as installing agents or creating users—only for *included* folders and items. KDS only harvests detailed information for *included* folders and items, minimizing the amount of data required to maintain synchronization with the domain.

Machine Group

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. You can also move a machine group and all of its associated machines to a different parent machine group within the same organization.

Machine ID / Group ID / Organization ID

Each **agent** *(page 35)* 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.

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.
- 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.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** *(page 36)* and the **agent** *(page 35)*. 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 creates and deletes machine roles. Machine roles determine what *machine users* see when they use Portal Access—a version of Live Connect—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 - Assign or remove machines for a machine role.
- Access Rights - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- Role Types - 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 35)* and active **machine ID / group ID** *(page 36)* account on the KServer. Each managed machine uses up one agent license.

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` is the organization of the service provider using the VSA.

Portal Access

Portal Access is a Live Connect 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. The function list the user sees during a **Portal Access** session is determined by the System > Machine Roles page. You can customize **Portal Access** sessions using the System > Customize > Live Connect page.

Probe Agent

KDS communicates with an Active Directory domain using a **probe agent**. The probe uses the industry standard LDAP protocol to safely and securely communicate with domain. Each probe agent must be a member of the domain it monitors. Probe deployment installs the extra functionality an agent requires to act as a probe.

Index

A

Agent Deployment Policy • 27
Agents • 35
Alert Policies • 31
Applying KDS Policies • 6
Audit Log • 33

C

Computer / Contact Policies • 28
Computers • 18
Configuration Prerequisites • 12
Configuring Agent Deployment Policy • 14
Configuring Alert Policies • 17
Configuring Computer Policies • 14
Configuring Contact Policies • 15
Configuring Probe Deployment • 13
Configuring Schedule and Status • 17
Configuring the KDS Domains Page • 12
Configuring User Policies • 16
Contact • 35
Contacts • 19

D

Deactivation / Reactivation • 11
Directory Services Overview • 1
Distinguished Name • 35
Domains • 25
Duplicate Exists • 35

E

Enabling Remote Portal Access in KDS • 8
Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords • 9

G

Getting Started • 2

H

How Agents are Installed Using KDS • 6
How Machine ID Accounts are Created in KDS • 7
How Machine Moves in Domains are Reflected in KDS • 7

I

Included / Excluded domain Folders and Items • 35

K

KDS System Requirements • 1

L

Licensing • 2

M

Machine Group • 36
Machine ID / Group ID / Organization ID • 36
Machine ID Template • 36
Machine IDs vs. Agents • 36
Machine Roles • 36
Making Changes to KDS Managed User Logons • 9
Managed Machine • 37
Managing a Synchronized Security Model • 3
Managing Multiple Domains • 3
Managing Remote Portal Access • 4

O

Org • 37

P

Portal Access • 37
Probe Agent • 37
Probe Alerts and Domain Alerts • 12
Probe Deployment • 26

S

Schedule and Status • 32
Setting KDS Policies • 4
Setting KDS Policies for Computers • 5
Setting KDS Policies for Users • 5
Setting Policies for Computers • 5
Synchronization • 10

U

Uninstalling • 12
User Policies • 29
Users and Portal Users • 21