Kaseya 2

Discovery

User Guide

Version 7.0

English

September 3, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Discovery Overview

Discovery (KDIS) discovers computers and devices on individual networks or entire domains. Once discovered agents can be installed on any computer or mobile device. If a discovered device cannot be installed with an agent, the device can still be identified using SNMP. SNMP-enabled devices can then be monitored using the **Monitor** module. Hardware audits of vPro-enabled machines can also be included in discovery scans. vPro-enabled machines can then be managed using the **Desktop Management** module. An **Assets** page provides a consolidated view of all computers and devices managed by the VSA, regardless of the method of discovery.

Discovery by domain enables the installation of agents on any machine known to an Active Directory domain. In addition **Discovery** can integrate VSA user logons and Portal Access logons with domain logons. **Discovery** can also create staff records based on contacts in the domain. Changes in the domain are synchronized with **Discovery** on a scheduled basis and do not require a VSA agent on the AD domain controller. **Discovery** uses the industry standard LDAP protocol to safely and securely communicate with Active Directory domains.

Discovery LAN Watch:

- Discovers computers and devices on individual networks.
- Deploys agents to discovered agent-less machines
- Identifies SNMP devices and vPro machines.
- Enables a device to be "promoted" to a managed **asset** *(page 6)*.

Discovery Domain Watch:

- 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 Discovery System Requirements.

Functions	Description
Overview	Displays the workflow of discovering computers and devices by network and by domain.
LAN Watch by Probe	Discovers devices on the same LAN as a selected "probe" machine.
LAN Watch by Network	Discovers computers and devices by LAN.
Discovered Devices - Grid View	Displays discovered computers and devices in table format.
Discovered Devices - Tile View	Displays discovered computers and devices in tile format.
Domain Watch	Configures the integration of Discovery with Active Directory domains.
Computers	Manages machine ID accounts created, based on applied Discovery computer policies, for all domains monitored by Discovery probes.

Contacts	Manages staff records created, based on applied Discovery contact policies, for all domains monitored by Discovery probes.
Users & Portal Users	Manages VSA users and Portal Access candidates created, based on applied Discovery group policies, for all domains monitored by Discovery probes.
View Assets	Provides a consolidated view of all "assets" managed by the VSA.
Settings	Sets options and default values that apply to the entire Discovery module.
Audit Log	Displays a log of Discovery module activities.

Discovery Module Requirements

Kaseya Server

- The Discovery 7.0 module requires VSA 7.0.

Directory Services

- Directory Services 1.2 is a feature set that can be licensed and enabled separately. The feature set provides advanced functionality in the Discovery module.

Network Probe

- Any Kaseya supported Windows, Apple or Linux agent operating system can be used. See **Agent Requirements** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm)*.

Domain Probe

- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1

Note: See general **System Requirements** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm)*.

Chapter 1

LAN Watch

In This Chapter

Getting Started with LAN Watch

The **LAN Watch by Network** and **LAN Watch by Probe** pages discover computers and devices on LANs. Any agent machine on a LAN can be selected as the "probe" machine for that LAN. Scanning a LAN using a probe machine discovers any device or machine with an IP address. Discovered devices can be workstations and servers without agents, SNMP devices and vPro-enabled machines. Discovered devices display on the following pages:

- Discovered Devices - Grid View
- Discovered Devices - Tile View

How LANs are Identified

A LAN is detected if a single computer on that LAN is installed with an agent. Detected LANs are identified consecutively as `LAN1`, `LAN2`, `LAN3`, etc. The name assigned to a LAN can be changed for easier recognition. Each LAN is distinguished by a unique combination of the following two items:

- The internal IP range shown in the **Scan Range** column, and
- The external IP address shown in the **Gateway** column.

The internal IP range shown in the **Scan Range** column is expressed as the starting IP address followed by the number of bits—for example, `/24`—representing the network portion of the IP address.

Using LAN Watch by Network

1. Select the row of a detected LAN in the upper panel.
2. Select **New** or **Edit** to set the scan properties. This includes the machine to serve as a probe machine. Windows, Mac and Linux agent machines can all serve as probe machines.
3. Optionally deploy agents to discovered computers by policy, using the **Agent Deployment Policy** tab in the lower panel.
4. Optionally create alerts for newly discovered types of computers and devices, using the **Alert Profiles** tab in the lower panel.
5. Optionally set asset policies for discovered computers and devices, using the **Asset Promotion** page.
6. Schedule a scan once or on a recurring basis using the **Schedule Scan** button, or run a scan immediately using the **Scan Now** button.
   - Optionally search for SNMP devices and vPro enabled machines using the Schedule Scan dialog.
   - A scan can be assigned to multiple LANs at the same time. Each LAN will execute the policies assigned for that LAN using the tabs in the lower panel.

Using LAN Watch by Probe

1. Select one or more machine IDs.

   > **Note:** Windows XP machines are not recommended as probe machines. NMAP is more reliable with later Windows operating systems.

2. Schedule a scan once or on a recurring basis using the **Schedule Scan** button, or run a scan immediately using the **Scan Now** button.
   - Optionally search for SNMP devices and vPro enabled machines using the **Schedule Scan** dialog.
   - A scan can be assigned to multiple machine IDs.

Duplicate LAN Ranges

Occasionally two LANs are listed on the **LAN Watch by Network** page with the same IP address range or overlapping IP address ranges. This condition is commonly caused by a device, router, or DHCP with a mis-configured subnet mask. When this happens:

- Discovery generates a system alert that displays on the Monitor > Alarm Summary page.
- Running **Discovery** scans on overlapping LANs will appear to 'move' machines back and forth between each LAN as they are re-discovered.

To avoid this behavior, network administrators can either:

- Reconfigure devices on their networks to correct the condition, or
- Set **Discovery** to "ignore" one of the networks.

Agent Deployment Policies tab

The **Agent Deployment Policies** tab of the **LAN Watch by Network** page sets policies for the deployment of agents on computers discovered on a selected network. For each type of operating system—for Windows, Mac and Linux—set the following:

- **Automatically install agents for <OS type> machines** - Check to enable.
- **Default Package** - For each type of OS, select an OS appropriate agent install package.
- **Designated Deployer Agent** - An agent machine on the same network used to deploy the agent.
- **User Name / Password / Confirm Password** - Enter an administrator credential that allows remote installation of an agent.

The policies you set also serve as defaults when deploying an agent *manually* using:

- Discovered Devices - Grid View
- Discovered Devices - Tile View
- Scan Results

Matching OS Type Requirement

Any OS type of computer that can support an agent can be used to scan a network: Windows, Mac or Linux. If an agent is deployed, **Discovery** automatically switches, if necessary, to a matching OS type machine on the same LAN. Since each type of OS can only deploy agents to target machines matching its own OS type, you must manually install at least one agent of each OS type—Windows, Mac and Linux—on a LAN to deploy agents automatically from then on to all three types of operating system.

Administrator Credential

The logon credential specified must have administrator rights on the remote selected machine.

- **If the target machine is on a domain**, the administrator credential must use the format `domain\administrator` or `administrator@domain`.
- **If the target machine is not on a domain**, then the administrator credential may require the format `local\administrator` or `<hostname>\administrator`.

- **If the target machine is a Linux machine**, the `root` username alone—without a hostname or domain—must be used.

Alerts Profiles tab

The **Alerting Profiles** tab of the **LAN Watch by Network** page sets **Discovery** alert policies for a selected LAN and device type: computer, mobile, network and firewall.

> **Note:** The **Alerts Active** checkbox in the **Edit** dialog enable and disables the **Discovery** alerts configured on this tab for a selected network.

Asset Promotion tab

The **Asset Promotion** tab of the **LAN Watch by Network** page configures the automatic promotion of devices to assets when the devices are discovered.

When an agent cannot be installed on a discovered device, the device can be "promoted" to a managed asset. For example, a router or printer may still require monitoring, even if an agent cannot be installed on the machine.

All managed assets must be assigned a machine group and organization. **Scoping rules** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4578.htm)* and **view filtering** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#214.htm)* features within the VSA depend on this assignment.

A discovered device can be manually promoted or demoted on the LAN Watch by Network page or LAN Watch by Probe page by toggling the / icon.

Scan Results

The **Scan Results** window displays the latest scan results for a network. The same window is displayed by clicking the icon on two different pages.

- Click the icon for a network the LAN Watch by Network page.
- Click the icon for an agent machine on the LAN Watch by Probe page.

> **Note:** There may be a delay displaying this page if a network scan is in process.

The **Scan Results** window has two tabs.

- Summary tab
- Devices tab

Discovered Devices

The **Discovered Devices - Grid View** page shows computers and devices discovered using LAN Watch by Probe and LAN Watch by Network. Use this page to install agents on discovered computers and mobile devices. You can also make discovered devices a managed asset, even if they cannot be installed with agent.

The **Discovered Devices - Tile View** page shows computers and devices discovered using LAN Watch by Network and LAN Watch by Probe. The scan results are *cumulative* from all probe machines. A record is not removed unless you delete it.

Tile View Format

Tile view displays each device on its own tile. A tile can include the following icons:

- - Click to display NMAP scan data.
- - Only displays if an agent is installed. Hover over this icon to display the **Quick View** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#9339.htm)* window. Click to launch **Live Connect** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4796.htm)*.
- / - Toggling this icon manually promotes or demotes a non-agent device to an asset.

 - Only displays if an agent is installed. The number of tickets created for this computer. Click to display the tickets in a ticket table.

 - Only displays if an agent is installed. The number of alarms created for this device or computer. Click to display the **Alarm Summary** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4112.htm)* page for this device.

 - Only displays if an agent is assigned a monitor set or if a SNMP device is assigned an SNMP set. Click to display the **Machine Status dashlet** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#2803.htm)* or **Device Status dashlet** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#2817.htm)*.

 - Hovering over a tile displays a pencil icon. You can edit the name of a discovered machine or device.

View Assets

The Audit > **View Assets** page is populated by **Discovery** scans of networks and domains.The **View Assets** page provides a consolidated view of all "assets" managed by the VSA. Types of assets include:

- **Agent managed machines and mobile devices** - Computers and mobile devices that have an agent installed on them are always considered managed assets and display on this page for as long as the agent is installed on them.
- **Devices promoted to an asset** - When an agent cannot be installed on a discovered device, the device can still be "promoted" to a managed asset and display on this page. For example, a router or printer may still require monitoring, even if an agent cannot be installed on the machine. There are many different types of non-agent device types that can be managed by the VSA: routers, switchers, printers, firewalls, etc. The **Make Asset** button on the Discovery > Discovered Devices - Grid View page enables you to "promote" a device to an asset. When you do the device begins displaying on this page. You can "demote" a asset using the **Demote Asset to Device** on this page. When you do, the asset is removed from this page.

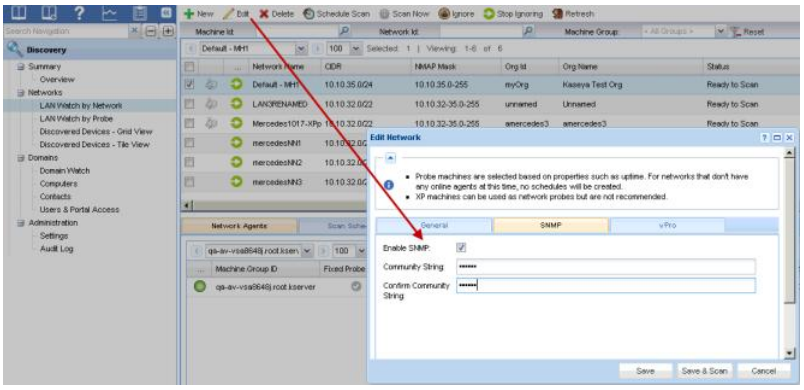
All managed assets are assigned a machine group and organization. **Scoping rules** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4578.htm)* and **view filtering** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#214.htm)* features within the VSA depend on this assignment.

- Multiple credentials can be defined for each asset. For agent assets, one of the credentials can be designated an agent credential and optionally used by **Policy Management** as an agent credential.
- **Service Desk** tickets can be optionally associated with assets listed on this page.

LAN Watch and SNMP

LAN Watch by Network or **LAN Watch by Probe** in the **Discovery** module uses an existing VSA agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran.

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



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

1. Select a machine ID on the same LAN as the SNMP devices you want to discover.
2. Check the **Enable SNMP** checkbox.
3. Enter a `community name` in the **Read Community Name** and **Confirm** fields.

   A community name is a credential for gaining access to an SNMP-enabled device. The default "read" community name is typically `public`, in all lower case, but each device may be configured differently. You may have to identify or reset the community name on the device directly if you're not sure what community name to use.
4. Click the **Schedule and Scan** button at the bottom of the **Edit Network** dialog. This will start the scan immediately.
5. Review discovered SNMP-enabled devices using the Monitor > Assign SNMP page.

LAN Watch and vPro

The Audit > View Assets > **vPro** tab displays hardware information about vPro-enabled machines discovered by enabling a vPro scan using the Edit Network dialog, then running **LAN Watch** *(http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#11552.htm)*. This information is only available if a machine's vPro credential is specified by the **LAN Watch**.

Types of hardware information returned by the vPro machine include:

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

Note: The **vPro** module provides **vPro management features** *(http://help.kaseya.com/webhelp/EN/vpro/7000000/index.asp#home.htm)*.

Chapter 2

Domain Watch

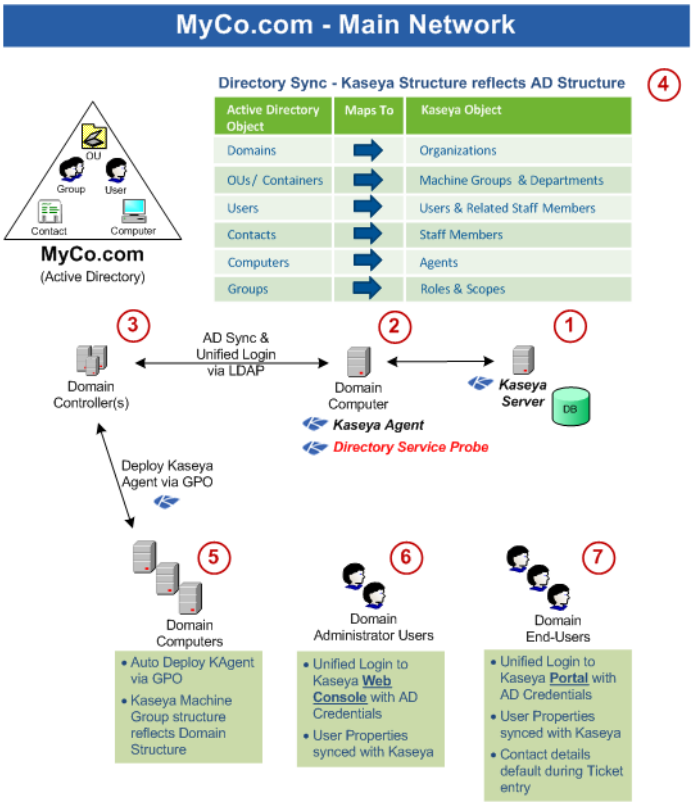
In This Chapter

Getting Started with Domain Watch

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

- 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).



- The application protocol used to communicate with the domain server is Lightweight Directory Access Protocol (LDAP).
- See OU/Container for more information about "organizational units".

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

These additional topics provide an overview of **Discovery** concepts.

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 as email, phone and other contact information need only be updated in the domain to update corresponding fields in the VSA.

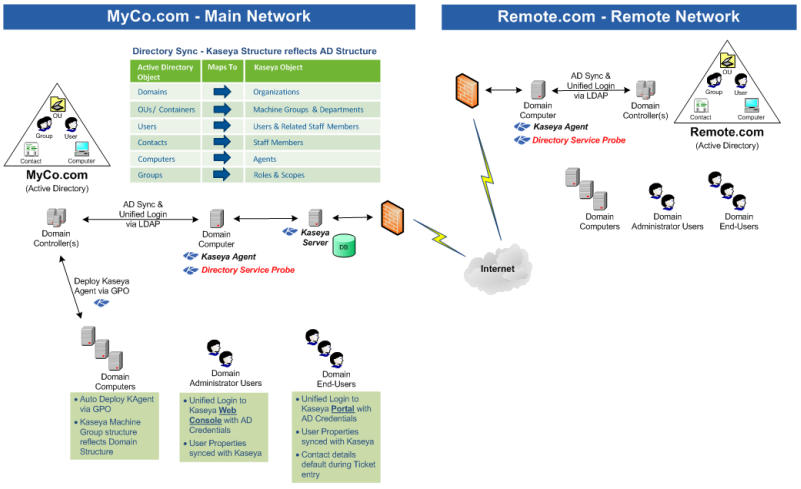
The security model created in the VSA by **Discovery** integration with the Active Directory domain results in the following mapping of objects.

Directory Sync - Kaseya Structure reflects AD Structure

Active Directory Object	Maps To	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

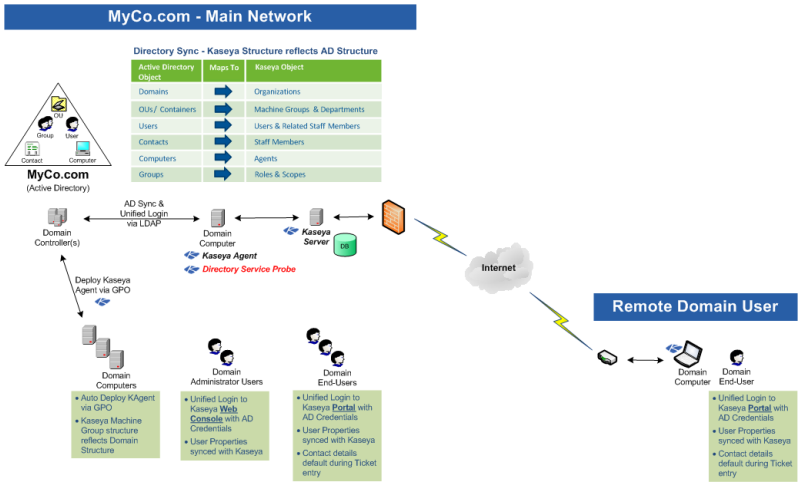
Discovery provides consolidated access throughout the VSA to **Discovery** managed domain computers, users and contacts, regardless of whether these domains have a "trust" relationship between them. For example, **Discovery** can provide a consolidated view of the domains of both a primary company and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



- Each **Discovery** 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

Discovery sets policies that enable users to use their domain credentials to logon remotely to their machines using 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.



Licensing

Discovery domains are licensed separately from agent licenses. **Discovery** domain license counts display on the **Licenses** tab of the System > **License Manager** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#2924.htm)* page.

A **Discovery** managed domain is a domain attached to an organization. A domain is attached to an organization when *activated* using the Domains > Domain Watch > Probe Deployment tab. A managed domain can be in one of following licensing states:

- **Unlicensed** - **Discovery** 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** - **Discovery** has been disabled because licensing for the entire module has expired.

The Directory Services Feature Set

Directory Services 1.2 is a feature set, licensed separately, that provides advanced functionality in the **Discovery** module.

Domain Policies	Domain policies can be can specified for multiple machines and users by: • OU/Container • Groups
Incremental Synchronization Activation/Deactivation	Provides incremental discovery and synchronization of domain controller data. Without Directory Services 1.2 only full discovery and synchronization is supported. Activation and Deactivation buttons display on the Domain Watch > Probe Deployment page, enabling and disabling incremental discovery and synchronization.
Auto Portal Access	Auto creates portal access to a machine, based on the person last logged on to the machine.

Contacts	Discovers and synchronizes domain contacts and VSA staff records. A domain contact contains information similar to a domain user, but a contact has no domain logon privileges. Directory Services 1.2 enables you to set policies that create VSA staff member records for newly discovered contacts in a domain and to keep the two records synchronized with each other. Creating a staff record using a Directory Services policy also creates a hierarchy of departments that reflects the OU/container hierarchy in the domain.
Users	• Enables and disables domain logons from the Directory Services module. • Resets the domain passwords. • Unlocks domain accounts.
Alerts	Provides alerts for new or changed computers, contacts, OU/containers, domains, groups, organizations, or users.

Setting Discovery Policies

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

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

- **Setting Discovery Policies for Computers** *(page 13)*
- **Setting Discovery Policies for Contacts** *(page 13)*
- **Setting Discovery Policies for Users** *(page 14)*

Setting Discovery Policies for Computers

The following **Discovery** *computer* policies can be set by OU/container or by individual computer. Setting a policy by computer has precedence over setting a policy by OU/container.

- 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 16)*.

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

Discovery computer policies are set using the Domains > Domain Watch > Policies > OU/Containers tab or Computers tab.

Setting Policies for Computers

The following **Discovery** *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 **Discovery** policy also creates a hierarchy of departments that reflects the OU/container hierarchy in the domain.

Discovery contact policies are set using the Domains > Domain Watch > Policies > OU/Containers tab.

Setting Discovery Policies for Users

Discovery 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 **Discovery** *user* policies can be set by (user) group or set by individual user.

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 16)* for details.
4. `Create VSA Users` - Creates VSA user logons for domain users listed in this group.

Discovery user policies are set using the Domains > Domain Watch > Policies > Groups tab or Users tab.

Applying Discovery Policies

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

- Computers
- Contacts
- Users & Portal Users

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 **Discovery**.

- **How Agents are Installed Using Discovery** *(page 14)*
- **How Machine ID Accounts are Created in Discovery** *(page 15)*
- **How Machine Moves in Domain are Reflected in Discovery** *(page 16)*
- **Enabling Remote Portal Access in Discovery** *(page 16)*
- **Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords** *(page 17)*
- **Making Changes to Discovery Managed User Logons** *(page 18)*
- **Supported Domain Logon Formats** *(page 18)*

How Agents are Installed Using Discovery

All agents installed on domain machines using **Discovery** 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 **Discovery** 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.

Discovery uses two methods for installing agents.

Method 1 - Agent Installs Using Kconnect

Applies to both network installs and domain installs.

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 by Network to remotely install an agent. The agent install package is downloaded from the Kaseya Server 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

Applies only to domain installs. Both method 1 and method 2 are initiated at the same time for a domain install. If an install using one method has already succeeded, any subsequent attempt to install an agent is canceled.

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 **Discovery** 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.*

Updating the Install Package on the Domain Controller

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 Discovery

The creation and grouping of machine ID accounts using **Discovery** 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 **Discovery**. The organization selected determines the organization assigned to *newly created machine ID accounts* when installed using **Discovery**.

- 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 **Discovery** creates an "empty" machine ID template 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 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 Discovery > Computers page then click the **Synchronize Machines** button.

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

How Machine Moves in Domains are Reflected in Discovery

When a machine is *moved* to a new OU in the domain, the effect it has in **Discovery** depends on the policies selected using the Discovery > Domains > Domain Watch > Policies > OU/Containers or Computers. **Discovery** 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 Domains > Computers > **Synchronize Machines** button.
- **From Excluded to Excluded** - No change is made in the VSA.

Enabling Remote Portal Access in Discovery

Portal Access enables the end-user of a managed machine to remotely logon to that machine. Only one end-user of a machine can have Portal Access to that machine at a time. The end-user must have previously logged onto the machine locally at least once. **Discovery** supports both manual and automatic Portal Access assignment. For more information see:

- **Managing Remote Portal Access** *(page 12)*

Automatic Portal Access Assignment

When a domain user logs on to a domain machine, *both the domain machine and the domain user* must be designated as **Discovery portal candidates** to enable the user to be *automatically assigned* as the **Portal Access** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#438.htm)* user of that machine.

Manual Portal Access Assignment

Discovery 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.

Portal Access Using Discovery

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

- 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 OU/Containers 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.

  Note: *The user can only be manually assigned the* **Portal Access** *user of a machine—using the* Users & Portal Users *page—if the user was the last user logged on to that machine.* The list of eligible machines are listed in the **Last Logged-onto Machines** field in the lower panel of this same page.

- 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.

Enabling/Disabling Domain Users Accounts or Resetting Domain User Passwords

Note: The enabling and disabling of domain logons, the resetting of domain passwords and the unlocking of domain accounts is only available if the **Directory Services** feature set is enabled.

When the **Discovery** > 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 **Discovery** managed user or enable/disable that user using the System > **Users** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4576.htm)* 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 Discovery Managed User Logons

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

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

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

> **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 **Discovery** 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 **Discovery** user policy is applied.

Demote a VSA User to a Portal Access User

- Delete the VSA user logon only.
- Modify **Discovery** 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 **Discovery** user policy is applied.

Supported Domain Logon Formats

The following domain logon formats are supported using **Discovery**, for both VSA users and Portal Access users.

Format	Field	Full DNS Domain Name Logons*	Pre-Windows 2000 Domain Name Logons**
Domain Back Slash	Username	*ITservices.acme.com\william*	*ITservices\william*
	Password	********	********

	Domain		
Domain Forward Slash	Username	*ITservices.acme.com/william*	*ITservices/william*
	Password	********	********
	Domain		
Separate Domain	Username	*william*	*william*
	Password	********	********
	Domain	*ITservices.acme.com*	*ITservices*
Email Style Domain	Username	*william@ITservices.acme.com*	*william@ITservices*
	Password	********	
	Domain		

** The Full DNS domain name is also known as the User Principal Name (UPN) suffix.*

*** The Pre-Windows 2000 domain name is also known as the NetBIOS Domain Name.*

Synchronization

Synchronization refers to the updating of **Discovery** with data harvested from an Active Directory domain. The following **Discovery** events trigger synchronization between **Discovery** 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 17)*.

Previews

When the **Discovery** probe is installed, the first task the probe performs is a **preview**. A preview updates **Discovery** 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

> **Note:** Incremental synchronization is only available if the **Directory Services feature set** *(page 12)* is enabled.

After the probe is installed —and typically before **Discovery** policies are even set—a **Discovery** 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 **Discovery** 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 **Discovery** 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 **Discovery**. 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 KDIS policies** *(page 14)*, and are equivalent to a *full* synchronization. This ensures applied policies affect *all* included domain computers, users and contacts that may exist at that time, regardless of any synchronizations that may have occurred before.

Full Synchronization

The **Discovery** probe accumulates domain *changes* in real time. If the connection between the **Discovery** 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 21)* and schedule a recurring *full* **synchronization** *(page 19)*. *If a probe alert is triggered, consider running a full synchronization immediately.*

A full synchronization provides **Discovery** 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.

Activation / Deactivation

Activation and **Deactivation** buttons display on the Domain Watch > **Probe Deployment** tab, but only if the **Directory Services Feature Set** *(page 12)* is installed.

- **Activation** - Enables incremental discovery and synchronization of domain controller data. Activating a probe on a domain computer *deactivates* any other probe on that same domain, without loss of data.

  Note: Activation is not required to run full sync on the Domain Watch > Schedule and Status tab.

- **Deactivation** - Disables 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.

Uninstalling the Probe and Detaching the Org

You associate an organization with a domain when a probe is installed. After the install, the association with the organization cannot be changed without uninstalling the probe and detaching the probe. This prevents creating duplicate users, staff and computer records in multiple organizations.

Uninstalling and detaching the org clears all records for that domain in the Computers, Contacts and Users & Portal Users 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.

Probe Alerts and Domain Alerts

Note: Alerts are only available if the **Directory Services feature set** *(page 12)* is enabled.

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 **Discovery** is no longer valid.
- The probe cannot communicate with the domain controller.

Warning: The **Discovery** probe accumulates domain *changes* in real time. If the connection between the **Discovery** 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 21)* and schedule a recurring *full* **synchronization** *(page 19)*. *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 Discovery Domains Page

The following topics provide a step-by-step procedure for configuring the Discovery > Domain Watch page.

Configuration Prerequisites

1. Identify the domain administrator credentials for the Active Directory domain you intend to integrate with the VSA. **Discovery** 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 **Discovery** 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 Domain Watch page until at least one domain computer has an agent installed on it.

Configuring Probe Deployment

Note: No tabs display unless a domain row in the upper panel is selected. At least one agent must be installed on a domain computer to see that domain row displayed in the upper panel.

1. Click the Discovery > Domains > Domain Watch > Probe Deployment tab.
2. Select the row of the **Domain Name** in the upper panel 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 panel.
   - 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 **Discovery** policies, these domain computers will all be displayed in the lower pane.
3. Select one of the machines in the lower panel.
   - Click the enabled **Install** button in the lower panel.
4. The first thing the **Install** dialog asks you to enter is a credential. **Discovery** 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 **Discovery** to just the privileges listed above.

5. Click the **Verify and Set Credentials** button.
   - If the credential is valid, the dialog displays a second **Install** button.
6. Optionally filter the scan performed by the probe machine using the **Filter String**. Useful for large domains. Use distinguished name notation. For example, `CN=Users,DC=myDomain,DC=com`
7. The **Install** dialog asks you to specify a **unique** VSA organization for each domain integrated with **Discovery**.
   - 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.
   - After the install, the association with the organization cannot be changed without **Uninstalling the Probe and Detaching the Org** *(page 21)*. This prevents creating duplicate users, staff and computer records in multiple organizations.
8. Click the **Install** button in the dialog. The dialog closes.
   - **Discovery** 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 **Policies** tabs 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`.

> **Note:** **Activation** and **Deactivation** buttons only display if the **Directory Services Feature Set** *(page 12)* is installed.

9. Reselect the probe agent row. Click the **Activate** button in the lower panel. 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.

> **Note:** If a probe has already been installed and activated once, the **VSA Organization** field may be disabled. Click the **Uninstall and Detach Org** button. Then click the **Activate** button to enable the list and pick a different org. See **Activation / Deactivation** *(page 20)* for issues to consider before *deactivating* a probe.

   - Set a **incremental synchronization interval** *(page 19)* for synchronization of data between the domain and **Discovery** The default is 60 minutes. This option is only available if the **The Directory Services Feature Set** *(page 12)* is installed.
   - 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 **Discovery** policies. This ensures all changes in the domain are monitored while you continue with your configuration.

Configuring Agent Deployment

1. Click the **Discovery** > Domains > Domain Watch > Agent Deployment 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.*

     > **Note:** Kaseya recommends leaving this checkbox *blank* until all Policies are configured for a domain for the first time.

   - **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 a Windows-based agent install package to use with the selected domain.

     > **Note: Domain Watch** does not support installing agents on Linux or Apple machines. Agents must be installed on domain Linux machines and domain Apple machines outside of **Domain Watch**. See **How Agents are Installed Using Discovery** *(page 14)*.

3. Click the **Save** button to close this dialog.

Configuring OU/Container Policies

> **Note:** The **OU/Containers** tab and **Groups** tab only display if the **Directory Services feature set** *(page 12)* is enabled. Policies for contacts are configured using the **OU/Containers** tab.

1. Click the Discovery > Domains > Domain Watch > Policies > OU/Containers.
   - 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* 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 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 account created for a domain computer in the Computers 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 16)*.
- 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 **Discovery** 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:** You do not need to **Apply Changes** until all **Policies** tabs have been configured. Clicking the **Apply Changes** button on any tab applies **Discovery** policy changes for all tabs at the same time.

Configuring Contact Policies

> **Note:** The **OU/Containers** tab and **Groups** tab only display if the **Directory Services feature set** *(page 12)* is enabled. Policies for contacts are configured using the **OU/Containers** tab.

1. Click the Discovery > Domains > Domain Watch > Policies > Computers 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* 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:** You do not need to **Apply Changes** until all **Policies** tabs have been configured. Clicking the **Apply Changes** button on any tab applies **Discovery** policy changes for all tabs at the same time.

Configuring Computer Policies

1. Click the Discovery > Domains > Domain Watch > Policies > Computers.
   - Use this tab to select *individual* domain computers you want to install a Kaseya agent on. This tab has precedence over policies set on the **OU/Containers** tab.
   - Each computer 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.
2. Select the **Computers Policy** button.
   - Set the computer policy for the selected machine to Include or Do Not Include.
   - Optionally set the **Computer Machine Group Override** drop-down list. This specifies the machine group to use when an agent is installed on this computer.
3. Click **Save**.
   - The **Probe Status** displays Activated and the **Policy Status** displays Modified because the policy changes just made have not yet been applied.

> **Note:** You do not need to **Apply Changes** until all **Policies** tabs have been configured. Clicking the **Apply Changes** button on any tab applies **Discovery** policy changes for all tabs at the same time.

Configuring Group Policies

> **Note:** The **OU/Containers** tab and **Groups** tab only display if the **Directory Services feature set** *(page 12)* is enabled. Policies for contacts are configured using the **OU/Containers** tab.

1. Click the Discovery > Domains > Domain Watch > Policies > Groups tab.
   - **Discovery** user policies enable users to logon to the VSA or to **Portal Access** *(page 16)* 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 **Total Users** 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 Group Policy** button.
   - The **Group Policy** dialog displays, listing the **Member Users** in this group.
4. Select a **Member Group Policy.**
   - Each user group in **Discovery** 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*.

       > **Note:** *The user can only be manually assigned the* **Portal Access** *user of a machine—using the* Users & Portal Users *page—if the user was the last user logged on to that machine.* The list of eligible machines are listed in the **Last Logged-onto Machines** field in the lower panel of this same page.

     - ✓ `Create Staff and make Auto Portal Candidates` - Designates domain users in this user group as Portal Access candidates. See **Making Portal Access Candidates** *(page 16)* 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 the **Groups** tab and **Users** tab can be modified and reapplied multiple times. Successive changes will cause roles and scopes to *accumulate, rather than be replaced.* **Discovery** 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 **Discovery** policies for computers and contacts, click the **Apply Changes** button.

> **Note:** You do not need to **Apply Changes** until all **Policies** tabs have been configured. Clicking the **Apply Changes** button on any tab applies **Discovery** policy changes for all tabs at the same time..
>
> **Note:** See **Supported Domain Logon Formats** *(page 18)*.

Configuring User Policies

1. Click the Discovery > Domains > Domain Watch > Policies > Users tab.
   - **Discovery** user policies enable users to logon to the VSA or to **Portal Access** *(page 16)* 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 user.
3. Select the **Configure Users Policy** button.
   - The **Users Policy** dialog displays.
4. Select a **Member User Policy.**
   - Each domain user in **Discovery** can be assigned one of three different VSA logon policies.
     - ✓ `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*.

       > **Note:** *The user can only be manually assigned the* **Portal Access** *user of a machine—using the* Users & Portal Users *page—if the user was the last user logged on to that machine.* The list of eligible machines are listed in the **Last Logged-onto Machines** field in the lower panel of this same page.

     - ✓ `Create Staff and make Auto Portal Candidates` - Designates domain users in this user group as Portal Access candidates. See **Making Portal Access Candidates** *(page 16)* for details.
     - ✓ `Create VSA Users` - Creates VSA user logons for domain users listed in this user group.
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 the **Groups** tab and **Users** tab can be modified and reapplied multiple times. Successive changes will cause roles and scopes to *accumulate, rather than be replaced*. **Discovery** 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 have already defined policies for other tabs, click the **Apply Changes** button.

> **Note:** You do not need to **Apply Changes** until all **Policies** tabs have been configured. Clicking the **Apply Changes** button on any tab applies **Discovery** policy changes for all tabs at the same time.
>
> **Note:** See **Supported Domain Logon Formats** *(page 18)*.

Configuring Alerting Profiles

> **Note:** The **Alerting Profiles** tab only displays if the **Directory Services** **feature set** *(page 12)* is enabled.

1. Click the Discovery > Domains > Domain Watch > Alerting Profiles tab.
2. Enable all probe alerts.

> **Warning:** The **Discovery** probe accumulates domain *changes* in real time. If the connection between the **Discovery** 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 21)* and schedule a recurring *full* **synchronization** *(page 19)*. *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, 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, groups and users. You may need to review **Discovery** policies after creating or deleting one of these objects.

Configuring Schedule and Status

1. Click the Discovery > Domains > Domain Watch > Schedule and Status tab.
2. Enable full synchronization on a weekly basis.

> **Warning:** The **Discovery** probe accumulates domain *changes* in real time. If the connection between the **Discovery** 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 21)* and schedule a recurring *full* **synchronization** *(page 19)*. *If a probe alert is triggered, consider running a full synchronization immediately.*

Removing a Domain from Discovery Management

If you wish to remove a domain from **Discovery** management, consider deleting the following types of domain generated records from the VSA:

- Optionally delete any domain-generated machine ID template records using Agent > **Delete** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#541.htm)*. These are typically identified as belonging to the organization associated with the domain in **Discovery**.
- Optionally delete domain-generated VSA users using System > **Users** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4576.htm)*. Each domain-generated VSA username is prefixed with the name of the domain, using the following format: `domain/username`.
- Optionally delete domain-generated Portal Access user logons using the Agent > **Portal Access** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#438.htm)* page.
- Optionally delete the organization associated with the domain using System > Orgs/Groups/Depts/Staff > **Manage** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4017.htm)*.
  - An organization cannot be deleted if machine ID accounts are members of that organization.
  - For machine ID accounts you want to keep, use Agent > **Change Group** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#545.htm)* to move machine ID accounts to a machine group in another organization.
  - For machine ID accounts you don't want to keep, use Agent > **Delete** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#541.htm)* to uninstall the agents and delete the machine ID accounts.
- If you elect to keep the organization associated with the domain, optionally delete the staff records created for domain contacts in the organization, using the System > Orgs/Groups/Depts/Staff > Manage > **Staff** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#7018.htm)* tab.
- It is possible a dedicated scope was created using the Discovery > Domain > User Policies tab. This dedicated scope is initially assigned the same name as the organization associated with the domain. Optionally delete this dedicated scope.

Uninstalling Discovery

> **Note:** Before uninstalling the **Discovery** module, review **Removing a Domain from Discovery Management** *(page 30)*.

1. Deactivate and detach the organization
2. Uninstall the probe from the agent.
3. Uninstall the **Discovery** module from the Kaseya Server.

Index