Kaseya

Policy Management

User Guide

Version R94

English

April 19, 2017

Copyright Agreement

Contents

Policy Management Overview

The **Policy Management** (KPM) module manages *agent settings by policy*.

- Once policies are assigned to machines, machine groups or organizations, *policies are propagated automatically*, without further user intervention.
- Each policy comprises sub-categories of agent settings called *policy objects*.
- Policies can be assigned by machine ID, machine group, or organization. A view definition must be used to filter the machines affected by the policy.
- Changing a machine's association with a machine group, organization, or view, causes the appropriate policies to be automatically re-deployed.
- Multiple policies can be assigned to each machine. If policies conflict, policy assignment rules determine the policies that are obeyed or ignored.
- A compliance cycle checks that each machine is in compliance with applied policies. VSA users can check the status of each machine to ensure it is in compliance with applied policies.
- A policy can be overridden. A **Policy Management** policy override condition exists if agent settings for a machine have been set manually, outside of the **Policy Management** module. For example, making changes to the agent menu of a machine using the **Agent Menu** page in the **Agent** module sets up an override condition for that agent machine. **Policy Management** policies will be ignored from then on. Policy overrides can also be cleared.
- Policies can be imported and exported using System > **Import Center** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#6963.htm)*.
- A **System cabinet** *(page 36)* provides built-in policies that reflect best-practice solutions for common IT management tasks. Policies can be configured for an organization automatically using the **Systems Management Configuration setup wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9040000/index.asp#11220.htm)* and these System cabinet policies.

Additional Terms

- *Applying a policy* means the changes made to its policy objects are *marked for deployment*. Deployment means the applied changes are propagated to target machines, based on the deployment interval set using the **Settings** *(page 26)* page. Because deployment may take a while, the target machine might not be *in compliance* between the time the policy is applied and the policy is deployed.
- *Pending changes* are changes to policies or policy objects that have been saved, but not yet applied.

Configuration

1. Set general settings for the entire **Policy Management** module using the **Settings** *(page 26)* page.
2. Define agent setting policies using the **Policies** *(page 5)* page.
3. Apply policies to:
   - Organizations and machine groups using the **Organizations / Machine Groups** *(page 27)* page.
   - Individual machines using the **Machines** *(page 28)* page. You can also clear **Policy Management** policy overrides using this page, enabling applied policies to take effect.

     > **Note:** Policies will begin propagating after the policies are applied.
4. Monitor policy compliance using the **Policy Matrix** *(page 4)* page and **Dashboard** *(page 3)* page.
5. Monitor **Policy Management** activity using the **Logs** *(page 3)* page.

Creating Policies Based on Agent Templates

You can migrate agent settings managed by agent template to **Policy Management**. The **Import from Templates** button on the **Policies** *(page 5)* page creates a policy based on the agent settings supported by the Agent > **Copy Settings** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#547.htm)* page.

> **Note:** See KPM System Requirements.

Functions	Description
Overview	Illustrates the Policy Management workflow graphically.
Dashboard *(page 3)*	Provides a dashboard view of Policy Management activities.
Logs *(page 3)*	Displays a log of Policy Management module activity.
Policy Matrix *(page 4)*	Displays the policy status of all machines your scope authorizes you to see. A policy status icon displays in the left most column for every machine on this page.
Policies *(page 5)*	Defines agent settings by policy, including • Agent Menu • Alerts • Audit Schedule • Checkin • Credential • Distribute Files - This policy object is not available in a **SaaS** *(page 36)*-based VSA. • Event Log Settings • Kaseya Anti-Malware • Kaseya AntiVirus • Kaseya Security • Log History • Machine Profile • Monitor Sets • Patch File Source • Patch Procedure Schedule • Patch Reboot Action • Patch Settings • Patch Windows Automatic Update • Protection • Remote Control • Working Directory
Settings *(page 26)*	Schedules the interval for automatic deployment of all policies to all assigned machines.
Organizations / Machine Groups *(page 27)*	Assigns policies to organizations and machine groups.
Machines *(page 28)*	Assigns policies to individual machines.

Policy Management Module Minimum Requirements

Kaseya Server

- The Policy Management R94 module requires VSA R94.

> **Note:** See general **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9040000/reqs/index.asp#home.htm)*.

Dashboard

Policy Management > Dashboard

The **Dashboard** page provides a dashboard view of **Policy Management** activities, including:

- **Agent Status** - Displays a pie chart of policy compliance status, by agent count and by agent percentage. Click a pie slice to display an **Agent Status Detail Grid** of the policy compliance status of member machines. Within this window you can click the **Go to Policy Management Machines Screen** button to display the **Machines** *(page 28)* page and update policy assignments by individual machine.

  - `In Compliance Agents` - The agent settings for this machine match the settings of all policies assigned to this machine.

  - `Marked for Deployment Agents` - At least one policy assigned to this machine has been changed and is scheduled to be deployed.

  - `No Policy Agents` - No *applied* policies are assigned to this machine.

  - `Out of Compliance Agents` - At least one agent setting does not match at least one active policy assigned to this machine.

  - `Override Agents` - At least one agent setting does not match at least one active policy assigned to this machine, *due to a user override*. An override occurs when an agent setting is set manually by any VSA user anywhere in the system. If even a single agent setting is overridden in a policy assigned to a machine, no other agent settings in that policy are enforced on that machine. Other policies assigned to the same machine remain enforced.

- **Policy Status** - Displays a pie chart of policy status, by policy status count and percentage.
  - ➢ `Deployed Policies` - Policies deployed to at least one agent.
  - ➢ `Not Assigned Policies` - Policies unassigned to any agent.
  - ➢ `Unapplied Changes Policies` - Deployed policies with saved changes that have not yet been applied. These policies display with a icon on the **Policies** *(page 5)* page.

- **Pending Events** - Lists policy changes or manual overrides that have not yet been processed. Pending events are processed at regular intervals, so usually this grid does not contain much data.

Logs

Policy Management > Logs

The **Logs** page displays a log of **Policy Management** module activity by:

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

This table supports **selectable columns, column sorting, column filtering and flexible columns widths** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#6875.htm)*.

Policy Matrix

Policy Management > Policy Matrix

The **Policy Matrix** page displays the policy status of all machines your scope authorizes you to see. A policy status icon displays in the left most column for every machine on this page.

Policy Details

Hovering the cursor over a policy status icon on this page displays a **Policy Details** window. The **Policy Details** window displays two tabs.

- **Policy Object Status Details** - Lists every policy and policy *category applied* to a selected machine.
- **Machine Effective Policy Settings** - Lists every policy *setting in effect* for a selected machine. Since more than one policy can be applied to a machine, some applied settings may be ignored, based on **policy assignment rules** *(page 27)*.

Table Columns

- **(Policy Status Icons)**
  - `In Compliance` - The agent settings for this machine match the settings of all policies assigned to this machine. No user action is required.
  - `Marked for Deployment` - At least one policy assigned to this machine has been changed and is scheduled to be deployed. No user action is required.
  - `No Policy Attached` - No *applied* policies are assigned to this machine. Consider assigning *applied* policies to this machine.
  - `Out of Compliance` - At least one agent setting does not match at least one active policy assigned to this machine. Use the **Policy Details** window to identify the specific policies and settings that are causing the mismatch.
  - `Overridden` - At least one agent setting does not match at least one active policy assigned to this machine, *due to a user override*. An override occurs when an agent setting is set manually by any VSA user anywhere in the system. Use the **Policy Details** window to confirm the override of specific policies and settings are correct. If even a single agent setting is overridden in a policy assigned to a machine, no other agent settings in that policy are enforced on that machine. Other policies assigned to the same machine remain enforced.
  - `Inactive` - *This policy status only displays in the* **Policy Details** *window.* When multiple policies are assigned to a machine and agent settings conflict, **policy assignment rules** *(page 27)* determine which agent settings are obeyed and which agent settings are ignored. Ignored settings are identified as inactive. A machine can show an `In Compliance` policy status icon while the *Policy Details* windows shows specific agent settings in specific policies as `Inactive`. This is expected behavior. No user action is required.
- **Machine ID** - The machine ID a policy is assign to. Multiple will display for a machine ID, one row for each policy assigned to that machine ID.
- **Machine Group** - The machine group this machine ID is a member of.

- **Policy** - The policy assigned to this machine.
- **Policy Object Types** - The categories of agent settings assigned using this policy. A policy type in red text indicates that policy type is being overridden by a different policy and is not applied.
- **Associated By** - The type of object used to associate a machine with a policy: machine, machine group or organization.
- **View** - Views associated with a policy. A view *filters* the machines associated with a policy.
- **Active** - If Yes, the policy is active. Policies may be active or inactive, depending on their order or precedence, whether they have been overridden, or are out of compliance.

Policy Matrix Abbreviations

The following abbreviations display in the **Policy Object Types** column of the **Policy Matrix** page.

Abbreviation	Policy Object Type
AL	Alerts
AM	Agent Menu
AP	Agent Procedures
AS	Audit Schedule
CD	Credential
CI	Checkin
DF	Distribute Files
EL	Event Log Settings
KAM	Kaseya Anti-Malware
KAV	Kaseya Anti-Virus
KES	Kaseya Security
LG	Log History
MP	Machine Profile
MS	Monitor Sets
PFS	Patch File Source
PPS	Patch Procedure Schedule
PRA	Patch Reboot Action
PS	Patch Settings
PT	Protection
RC	Remote Control
SDP	Software Deployment Profile Assignment
SDR	Software Deployment Reboot Action
SDS	Software Deployment Scan Schedule
WD	Working Directory
WU	Patch Windows Automatic Update

Policies

Policy Management > Policies

The **Policies** page defines agent policies. Policies are organized by a **folder tree** *(page 6)*. A **System**

cabinet *(page 36)* provides built-in policies that reflect best-practice solutions for common IT management tasks. Policies can be configured for an organization automatically using the **Systems Management Configuration setup wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9040000/index.asp#11220.htm)* and these System cabinet policies.

> **Note:** When a policy is removed from an agent, the settings enforced by that policy remain in effect until they are changed manually or by assigning another policy.

Tabs

- **Settings** *(page 7)* - Agent policy settings are grouped by setting category in this tab. Click a setting category checkbox to specify the settings for that category.
- **Assigned Machine Groups** - The organizations and machines groups assigned to a policy display on this tab. A policy is assigned by organization or machine group using the **Organizations / Machine Groups** *(page 27)* page.
- **Assigned Machines** - *Use this tab to determine the machines that are members of a policy.* The list of machines displayed on this tab depends on the following:
  - The organizations or machine groups assigned this policy using the the **Organizations / Machine Groups** *(page 27)* page.
  - The individual machines assigned this policy using the **Machines** *(page 28)* page.
  - The view associated with this policy using the **Settings** *(page 7)* tab of the **Policies** page. A view associated with a policy filters machine membership in that policy.
    - ✓ The view associated with a policy is ignored if the policy is assigned *by machine* using the **Machines** page.
    - ✓ Views created by another user and not shared with you are not available for you to select in the **View** drop-down list. If another user shared a policy with you but the associated view was not shared with you, the policy is read-only.
    - ✓ The currently selected view in the **machine ID/group ID filter** at the top of the page. *The currently selected view only limits the display of machines on this tab, not whether machines are members of that policy.*

Creating Agent Policies

1. Select a folder in the middle pane.
2. Click the **Add Policy** button.
3. Enter a name and click **OK**.

   > **Note:** The policy name has a limit of 100 characters. Creating a name longer than 100 characters may cause the policy to time out and not be editable.

4. Define agent settings in the **Settings** tab of the right pane.
5. Click **Save** to save changes to the policy. A policy displays a yellow scroll 📜 icon if it has only been saved and not yet applied.
6. Click **Save and Apply** to save and apply settings for a selected policy. Apply means the settings are propagated to assigned machines. A confirmation message lets you **Apply Now** or **Allow scheduler to apply**, which applies changes using the deployment interval specified by the **Settings** *(page 26)* page.

Policies - Folder Tree

Policy Management > Policies > Folder Tree

Policies are organized using a folder tree in the middle pane. Use the following options to manage objects in this folder tree.

Always Available

- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon to apply filtering to the folder tree. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder tree.

When the Cabinet is Selected

- **Collapse All** - Collapses all branches of the folder tree.
- **Expand All** - Expands all branches of the folder tree.

When the Cabinet or a Folder is selected

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.

When a Folder is Selected

- **Add Policy** - Creates a new policy in the selected folder of the folder tree.
- **Apply Policies** - Applies all changes to all policies in a selected folder.
- **Import From Template** - Creates a policy based on the agent settings supported by the Agent > **Copy Settings** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#547.htm)* page. Use this feature to migrate machine templates to policies.
- **Rename** - Renames a selected folder.
- **Delete** - Deletes a selected folder.
- **Share** - **Shares** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#5537.htm)* a policy folder.

When a Policy is Selected

- **Save As** - Saves a policy under a new name.
- **Delete** - Deletes a selected policy.
- **Apply Policy** - Applies policy changes to a selected policy.

Policies - Settings tab

Policy Management > Policies > Settings tab

Agent policy settings are grouped by category in this tab. Click a category checkbox to specify the settings for that category.

Actions

- **Save** - Saves settings for a selected policy without propagating those settings to assigned machines. A policy displays a yellow scroll icon if it has only been saved and not yet applied.
- **Save and Apply** - Saves and applies settings for a selected policy. Apply means the settings are propagated to assigned machines. A confirmation message lets you **Apply Now** or **Allow scheduler to apply**, which applies changes using the deployment interval specified by the **Settings** *(page 26)* page.
- **Cancel** - Cancels changes made to settings without saving or applying them.

Heading

- **Name** - The name of a policy.
- **Description** - The description of a policy.

- **View** - A view definition associated with the policy. Once a policy is assigned to a view definition, the policy only applies to machines that are members of that view.
    - Assigning a policy to a view on the Policies page is *required* to assign a policy using the **Organizations/Machine Groups** *(page 26)* page. *This prevents the unintentional assignment of a policy to all machines in the VSA.* A policy without a specified view displays as a red scroll icon in the policy tree of the **Organizations/Machine Groups** page, indicating that it cannot be assigned. A folder with a red exclamation mark icon displays in the policy tree if it contains at least one policy without a specified view. When assigning an entire folder of policies to an organization or machine group, policies without a specified view are ignored.
    - Assigning a policy to a view is *not required* if the policy is only assigned using the **Machines** *(page 28)* page.
    - Views created by another user and not shared with you are not available for you to select in the **View** drop-down list. If another user shared a policy with you but the associated view was not shared with you, the policy is read-only.

Setting Categories

- **Policies - Settings tab - Agent Menu** *(page 9)*
- **Policies - Settings tab - Agent Procedures** *(page 9)*
- **Policies - Settings tab - Alerts** *(page 9)*
- **Policies - Settings tab - Audit Schedule** *(page 10)*
- **Policies - Settings tab - Check-in** *(page 11)*
- **Policies - Settings tab - Credential** *(page 12)*
- **Policies - Settings tab - Distribute File** *(page 13)* - This policy object is not available in a **SaaS** *(page 36)*-based VSA.
- **Policies - Settings tab - Event Log Settings** *(page 13)*
- **Policies - Settings tab - Kaseya Anti-Malware (Classic)** *(page 14)*
- **Policies - Settings tab - Kaseya Antivirus (Classic)** *(page 15)*
- **Policies - Settings tab - Kaseya Security** *(page 15)*
- **Policies - Settings tab - LAN Cache** *(page 15)*
- **Policies - Settings tab - Log History** *(page 15)*
- **Policies - Settings tab - Machine Profile** *(page 16)*
- **Policies - Settings tab - Monitor Sets** *(page 16)*
- **Policies - Settings tab - Patch File Source** *(page 17)*
- **Policies - Settings tab - Patch Procedure Schedule** *(page 18)*
- **Policies - Settings tab - Patch Reboot Action** *(page 19)*
- **Policies - Settings tab - Patch Settings** *(page 20)*
- **Policies - Settings tab - Patch Windows Automatic Update** *(page 21)*
- **Policies - Settings tab - Protection** *(page 21)*
- **Policies - Settings tab - Remote Control** *(page 22)*
- **Policies - Settings tab - Software Deployment Profile Assignment** *(page 23)*
- **Policies - Settings tab - Software Deployment Reboot Action** *(page 23)*
- **Policies - Settings tab - Software Deployment Scan Schedule** *(page 24)*
- **Policies - Settings tab - Suspend Alarms** *(page 24)*
- **Policies - Settings tab - Update List by Scan** *(page 25)*
- **Policies - Settings tab - Working Directory** *(page 25)*

Policies - Settings tab - Agent Menu

Policy Management > Policies > Settings tab > Agent Menu checkbox

The **Agent Menu** category assigns **agent menu** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#450.htm)* settings to a policy.

- **Enable Agent Icon** - Check to display the agent icon in the system tray of the managed machine. Uncheck to hide the agent icon and prevent the use of agent menu options.
- **About <Agent>** - Check to enable the machine user to click this option to display the About box for the installed agent. The default option label `Agent` can be customized.
- **<Contact Administrator...>** - Check to enable the machine user to click this option to contact an administrator. The label `Contact Administrator...` can be customized.
  - **User Logon page** - Displays the User Portal page for this machine.
  - `use <mid> for machine ID, <gid> for group ID, <guid> for agent GUID` - Displays a custom URL. Use the variables provided to construct a URL to a custom website you have created to administrate machines. For example: `http://www.yourcompany.com/?agentguid=<guid>` could display a website page you have created specific to an agent guid. Alternatively you could use the `<gid>` variable to construct a shared URL for all machines using the same machine group.
- **<Your Company URL...>** - Check to enable the machine user to click this option to display the URL specified in the corresponding URL field.
- **Disable Remote Control** - Check to enable the machine user click this option to *disable* remote control on the user's managed machine.
- **Set Account...** - Check to enable the machine user to click this option to display their machine ID.group ID.organization ID and to change the Kaseya Server address the agent checks into. The new IP address you enter must point to a working VSA, or else the IP address change will not take effect.
- **Refresh** - Check to enable the machine user to initiate an immediate full check-in.
- **Exit** - Check to enable the machine user to terminate the agent service on the managed machine.

Policies - Settings tab - Agent Procedures

Policy Management > Policies > Settings tab > Agent Procedure checkbox

The **Agent Procedures** category assigns **agent procedures** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2845.htm)* to a policy.

> **Note:** When multiple policies are assigned to the same machine all assigned agent procedures in all assigned policies are deployed to that machine.

- **Add Procedure** - Adds and schedules an agent procedure.
- **Remove Procedure** - Removes a selected agent procedure.

Policies - Settings tab - Alerts

Policy Management > Policies > Settings tab > Alerts checkbox

The **Alerts** category assigns standard alert notifications to a policy. **Each type of alert has different configuration settings** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2187.htm)*.

> **Note:** When multiple policies are assigned to the same machine all assigned *event log alerts* in all assigned policies are deployed to that machine. For all other types of alerts, only one policy can be in effect at any one time.
>
> **Note:** The email recipients field for any of these alerts may make use of **tokens** *(page 37)*.

- **Add Alert**
  - The **Alerts - Agent Status** page alerts when an agent is offline, first goes online, or someone has disabled remote control on the selected machine.
  - The **Alerts Application Changes** page alerts when a new application is installed or removed on selected machines.
  - The **Alerts - Get File** page alerts when a procedure's **getFile()** or **getFileInDirectoryPath()** command executes, uploads the file, and the file is now different from the copy previously stored on the Kaseya Server. If there was no previous copy on the Kaseya Server, the alert is created.
  - The **Alerts - Hardware Changes** page alerts when a hardware configuration changes on the selected machines. Detected hardware changes include the addition or removal of RAM, PCI devices, and disk drives.
  - The **Alerts - Low Disk** page alerts when available disk space falls below a specified percentage of free disk space.
  - The **Event Log Alerts** page alerts when an event log entry for a selected machine matches a specified criteria. After selecting the **event log type**, you can filter the alert conditions specified by **event set** and by **event category**.
  - The **Alerts - Agent Procedure Failure** page alerts when an agent procedure fails to execute on a managed machine.
  - The **Alerts - Protection Violation** page alerts when a file is changed or access violation detected on a managed machine.
- **Remove Alert** - Removes a selected alert.

Policies - Settings tab - Audit Schedule

Policy Management > Policies > Settings tab > Audit Schedule checkbox

The **Audit Schedule** category assigns schedules for a **Latest Audit, Baseline Audit and System Audit** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#222.htm)* to a policy. Each type of audit displays the same three scheduling options.

- **Edit Schedule** - Edits an existing audit schedule. Schedule a task once or periodically. Each type of recurrence—Once, Minutes, Hourly, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. Options can include:
  - **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.
  - **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. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
  - **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. Applies only to recurring schedules, a 'Once' schedule always executes the next time the agent is online.

  - **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-network or vPro and another managed system on the same network.
  - **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.
- **Reset** - A schedule for this type of audit is not set for this policy. If this same type of audit has a schedule defined in a lower priority policy it is *allowed* to take effect.
- **None** - A schedule for this type of audit is not set for this policy. If this same type of audit has a schedule defined in a lower priority policy it is *not allowed* to take effect.

Policies - Settings tab - Checkin

Policy Management > Policies > Settings tab > Checkin checkbox

The **Checkin** category assigns agent **check-in** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#243.htm)* settings to a policy.

Primary KServer

Enter the IP address or fully qualified host name of the machine ID's primary Kaseya Server. This setting is displayed in the **Primary KServer** column.

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

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

Primary Port

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

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

Secondary KServer

Enter the IP address or fully qualified host name of the machine ID's secondary Kaseya Server. This setting is displayed in the **Secondary KServer** column.

Secondary Port

Enter the port number of either the secondary Kaseya Server or a virtual system server. This setting is displayed in the **Secondary KServer** column.

Check-In Period

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

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

Bind to Kserver

If checked, the agent is bound to a **unique Kaseya Server ID**. Bound agents cannot check-in successfully unless the unique Kaseya Server ID they are bound to using the Agent > Check-in Control page matches the unique ID assigned to the Kaseya Server using the System > Configure > **Change ID** option. Prevents IP address spoofing from redirecting agent check-ins. A lock 🔒 icon in the paging areas shows the agent is bound. To *unbind* agents, select machines IDs, ensure **Bind to Kserver** is unchecked and click **Update**. The lock 🔒 icon no longer displays for selected machines.

Bandwidth Throttle

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

Warn if multiple agents use same account

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

Warn if agent on same LAN as KServer connects through gateway

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

> **Note:** Agents on the same LAN as the Kaseya Server should specify the internal IP address shared by both the agent and the Kaseya Server on the Check-In Control page.

Policies - Settings tab - Credential

Policy Management > Policies > Settings tab > Credential checkbox

The **Credential** category assigns an agent **credential** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* to a policy. *Many policies require an agent credential to execute successfully.*

> **Warning:** **Policy Management** ignores agent credentials specified using the Agent > **Manage Agents** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#250.htm)* page.

- **Use Managed Credential** - If checked, requires a credential be specified for any organization or machine assigned this policy using the Audit > Manage Credentials (http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#11364.htm) page.
- **Username** - Enter the username for the credential. Typically this a user account.
- **Password** - Enter the password associated with the username above.
- **Domain**
  - **Local user account** - Select this option to use a credential that logs into this machine locally, without reference to a domain.
  - **Use machine's current domain** - Create a credential using the domain name this machine is a member of, as determined by the latest audit. This makes it easier to **Select All** and rapidly set a common username/password on multiple machines, even if selected machines are members of different domains.
  - **Specify domain** - Manually specify the domain name to use for this credential.

Policies - Settings tab - Distribute Files

Policy Management > Policies > Settings tab > Distribute Files checkbox

The **Distribute Files** category **distributes files** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* stored on the Kaseya Server to machines assigned this policy.

> **Note:** The **Distribute File** policy object in is not available in a **SaaS** *(page 36)*-based VSA.

Select server file

Select a file to distribute to managed machines. These are the same set of files managed by clicking the **Manage Files...** link on this page.

> **Note:** The only files listed are your own private managed files or shared managed files. If another user chooses to distribute a private file you can not see it.

Specify full path and filename to store file on remote machine

Enter the path and filename to store this file on selected machine IDs.

Policies - Settings tab - Event Log Settings

Policy Management > Policies > Settings tab > Event Log Settings checkbox

The **Event Log Settings** category specifies the **event log types and categories** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3713.htm)* used to specify event log alerts.

To specify **Event Log Settings**:

1. Click an event log type in the **Available** list box. Hold down the [Ctrl] key to click multiple event log types.
2. Click **>** to add event log types to the **Selected** list box. Click **<** to remove event log types from the **Selected** list box.
3. Check one or more event categories:
   - **Error**
   - **Warning**
   - **Information**

- **Success Audit**
- **Failure Audit**
- **Critical** - Applies only to Vista, Windows 7 and Windows Server 2008
- **Verbose** - Applies only to Vista, Windows 7 and Windows Server 2008

Policies - Settings tab - Kaseya Anti-Malware

Policy Management > Policies > Settings tab > Kaseya Anti-Malware checkbox

The **Kaseya Anti-Malware** category assigns a **Anti-Malware profile** *(http://help.kaseya.com/webhelp/EN/AM/9040000/index.asp#33928.htm)* and **alert profile** *(http://help.kaseya.com/webhelp/EN/AM/9040000/index.asp#33935.htm)* to a policy. Machines assigned this profile will be installed with the **Anti-Malware** client if it is not already installed and assigned the selected profile.

> **Note:** Machines will reboot during the installation process. Once the install process has been initiated, it cannot be stopped.

- **Profile** - Selects the **Anti-Malware** profile to assign to this policy.
- **Alert Profile** - Selects the **Anti-Malware** alert profile to assign this policy. Alert profiles are applied to both **Antivirus** and **Anti-Malware** client installs.

Policies - Settings tab - Kaseya Anti-Malware (Classic)

Policy Management > Policies > Settings tab > Kaseya Anti-Malware (Classic) checkbox

The **Kaseya Anti-Malware (Classic)** category assigns a **Anti-Malware (Classic) profile** *(http://help.kaseya.com/webhelp/EN/KAM/9040000/index.asp#13280.htm)* to a policy. Machines assigned this policy must already have the **Anti-Malware (Classic)** client installed.

- **Profile** - Selects the **Anti-Malware (Classic)** profile to assign to this policy.

Policies - Settings tab - Kaseya Antivirus

Policy Management > Policies > Settings tab > Kaseya Antivirus checkbox

The **Kaseya Antivirus** category assigns a **Antivirus profile** *(http://help.kaseya.com/webhelp/EN/AV/9040000/index.asp#33906.htm)* and **alert profile** *(http://help.kaseya.com/webhelp/EN/AV/9040000/index.asp#33901.htm)* to a policy. Machines assigned this profile will be installed with the **Antivirus** client if it is not already installed and assigned the selected profile. **Antivirus** automatically assigns the appropriate profile type, server or workstation, for a machine.

> **Note:** Machines will reboot during the installation process. Once the install process has been initiated, it cannot be stopped.

- **Server Profile** - Selects the **Antivirus** server profile to assign to this policy.
- **Workstation Profile** - Selects the **Antivirus** workstation profile to assign to this policy.
- **Alert Profile** - Selects the **Antivirus** alert profile to assign this policy. Alert profiles are applied to both **Antivirus** and **Anti-Malware** client installs.

Policies - Settings tab - Kaseya Antivirus (Classic)

Policy Management > Policies > Settings tab > Kaseya Antivirus (Classic) checkbox

The **Kaseya Antivirus (Classic)** category assigns a **Antivirus (Classic) profile** *(http://help.kaseya.com/webhelp/EN/KAV/9040000/index.asp#13260.htm)* to a policy. Machines assigned this policy must already have the **Antivirus (Classic)** client installed. **Antivirus (Classic)** automatically assigns the appropriate profile type, server or workstation, for a machine.

- **Server Profile** - Selects the **Antivirus (Classic)** server profile to assign to this policy.
- **Workstation Profile** - Selects the **Antivirus (Classic)** workstation profile to assign to this policy.

Policies - Settings tab - Kaseya Security

Policy Management > Policies > Settings tab > Kaseya Security checkbox

The **Security** category assigns a **Endpoint Security profile** *(http://help.kaseya.com/webhelp/EN/KES/9040000/index.asp#2945.htm)* to a policy. Machines assigned this policy must already have the **Endpoint Security** client installed.

- **Profile** - Selects the **Endpoint Security** profile to assign to this policy.

Policies - Settings tab - LAN Cache

Policy Management > Policies > Settings tab > LAN Cache checkbox

The **LAN Cache** category assigns a **LAN Cache** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#9328.htm)* to a policy.

- **LAN Cache** - Selects the LAN Cache to assign to this policy.

Policies - Settings tab - Log History

Policy Management > Policies > Settings tab > Log History checkbox

The **Log History** category assigns **log entry settings** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#238.htm)* to a policy.

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

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

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

- **Sys Log** - The log of all System Check external systems.
- **Agent Uptime Log** - The uptime history log of agents.

Set days to keep monitoring logs for all machines

The following monitoring log settings are applied system-wide.

- **Event Log** - The log of all events. The events collected are specified in more detail using Agent > Event Log Settings.
- **Monitor Log** - The log of data collected by monitoring sets.
- **SNMP Log** - The log of all data collected by SNMP sets.
- **Agent Log** - The log of agent, system, and error messages.

Policies - Settings tab - Machine Profile

Policy Management > Policies > Settings tab > Machine Profile checkbox

The **Machine Profile** category assigns **machine profile** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#256.htm)* settings to a policy.

- **Contact Name** - Enter the name of the individual using the managed machine. This setting is displayed in the **Contact Name** column.
- **Contact Email** - Enter the email address of the individual using the managed machine. This setting is displayed in the **Contact Email** column.
- **Contact Phone** - Enter the phone number of the individual using the managed machine. This setting is displayed in the **Contact Phone** column.
- **Admin Email** - Enter the email address providing administrator support for this managed machine.This setting is displayed in the **Admin Email** column.
- **Language Preference** - The language selected in the **Language Preference** drop-down list determines the language displayed by an agent menu on a managed machine. The languages available are determined by the language packages installed using System > Preferences.
- **Machine Role** - The machine role to apply to selected machine IDs. Machine roles determine the Portal Access functions available to the machine user.
- **Notes** - Enter any notes about a machine ID account. Helpful information can include the machine's location, the type of machine, the company, or any other identifying information about the managed machine.
- **Show notes as tooltip** - If checked, **Edit Profile** notes are included as part of the tooltip that displays whenever the cursor hovers over a machine ID's check-in status icon.
- **Auto assign tickets** - 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 the **Auto assign tickets** checkbox checked.

Policies - Settings tab - Monitor Sets

Policy Management > Policies > Settings tab > Monitor Sets checkbox

The **Monitor Sets** category assigns **monitor sets** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#1938.htm)* to a policy.

> **Note:** When multiple policies are assigned to the same machine all assigned monitor sets in all assigned policies are deployed to that machine.

- **Add Monitor Set** - Adds and schedules monitor sets. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered.
  - **Create Alarm**
  - **Create Ticket**
  - **Run Script** `<agentprocedure>` on `<machineID>`
  - **Email Recipients** - Enter multiple addresses separated by commas.

    > **Note:** This field may make use of **tokens** *(page 37)*.
- **Remove Monitor Set** - Removes a selected agent procedure.

Policies - Settings tab - Patch File Source

Policy Management > Policies > Settings tab > Patch File Source checkbox

The **Patch File Source** category defines, by policy, the **file source** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#366.htm)* for patch executable files.

- **Copy packages to working directory on local drive with most free space** - Patches are downloaded, or copied from a file share, to the managed machine's hard disk. Several patches, especially service packs, may require significant additional local disk space to completely install. Check this box to download patches to the working directory, but use the drive on the managed machine with the most free disk space. Uncheck this box to always use the drive specified in **Working Directory** for the machine ID.
- **Delete package after install (from working directory)** - The install package is typically deleted after the install to free up disk space. Uncheck this box to leave the package behind for debugging purposes. If the install fails and you need to verify the Command Line switches, do not delete the package so you have something to test with. The package is stored in the **Working Directory** on the drive specified in the previous option.
- **Download from Internet** - Each managed machine downloads the patch executable file directly from the internet at the URL specified in Patch Location.
- **Pulled from system server** - First the Kaseya Server checks to see if it already has a copy of the patch file. If not, the new patch executable is downloaded automatically and stored on the Kaseya Server, then used for all subsequent distributions to managed machines. When a patch needs to be installed on a managed machine, this patch file is pushed to that machine from the Kaseya Server.

  > **Note:** The location for patch files stored on the Kaseya Server is `<Kaseya installation directory>\WebPages\ManagedFiles\VSAPatchFiles\`
- **Pulled from file server using UNC path** - This method is recommended if you support many machines on the same LAN. Patch files are downloaded to a local directory on a selected machine ID. The local directory on the machine ID is configured to be shared with other machine IDs on the same LAN. All other machine IDs on the same LAN use a UNC path to the shared folder located on the first machine ID.
  1. Identify an *agent machine* that will act as the *file server machine* for other machines on the same LAN.
  2. Create a share on the *file server machine* and specify the credential that will allow other machines on the same LAN to access it. This is done manually, outside of the **File Source** page.

3. Set an **agent credential** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* for the *file server machine* with the shared directory using Agent > Manage Agents. All other machines on the same LAN will use the credential set for the *file server machine* to access the shared folder.
4. Enter a UNC path to the share in the **Pulled from file server using UNC path** field. For example, `\\computername\sharedname\dir\`.

In the next three steps you tell the VSA which machine ID is acting as the *file server machine* and where the shared directory is located using local file format notation.

5. Use the **Machine Group Filter** drop-down list to select a group ID.
6. Select a machine ID from the **File share located on** drop-down list.
7. Enter a shared local directory in the **in local directory** field.

> **Note:** The value in the **in local directory** field must be in full path format, such as `c:\shareddir\dir`.

When a file is downloaded, the Kaseya Server first checks to see if the patch file is already in the file share. If not, the *file server machine* automatically loads the patch file either directly from the internet or gets it from the Kaseya Server.

8. **File Server automatically gets patch files from** - Select one of the following options:
   - ✓ **the Internet** - Use this setting when the *file server machine* has full internet access.
   - ✓ **the system server** - Use this setting when the *file server machine* is blocked from getting internet access.
9. **Download from Internet if machine is unable to connect to the file server** - Optionally check this box to download from the internet. This is especially useful for laptops that are disconnected from the company network but have internet access.

- **Pulled from LAN Cache** - Uses the Agent > LAN Cache and Agent > Assign LAN Cache pages to manage file sourcing for patch executable files.

Policies - Settings tab - Patch Procedure Schedule

Policy Management > Policies > Settings tab > Patch Procedure Schedule checkbox

The **Patch Procedure Schedule** category schedules two tasks that can be assigned to a policy.

- **Patch Scan** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#350.htm)* - Schedules scans to search for missing patches on each managed machine. Scanning takes very little resources and can be safely scheduled to run at any time of day. The scanning operation does not impact users at all.
- **Automatic Update** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#348.htm)* - Schedules an update of managed machines with Microsoft patches on a *recurring* basis. **Automatic Update** obeys both the **Patch Approval Policy** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3873.htm)* and the **Policies - Settings tab - Patch Reboot Action** *(page 19)* policy.

Patch Scan and **Automatic Update** each display the same three options and can be set separately within the same policy.

- **Edit Schedule** - Edits an existing task schedule. Schedule a task once or periodically. Each type of recurrence—Once, Minutes, Hourly, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. Options can include:
  - ➢ **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when

to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.

- **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. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
- **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. Applies only to recurring schedules, a 'Once' schedule always executes the next time the agent is online.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-network or vPro and another managed system on the same network.
- **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.

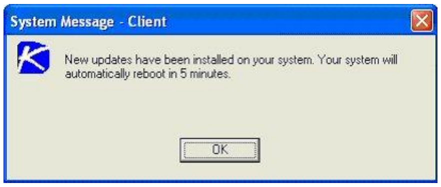
- **Reset** - A schedule for this task is not set for this policy. If this same task has a schedule defined in a lower priority policy it is *allowed* to take effect.
- **None** - A schedule for this task is not set for this policy. If this same task has a schedule defined in a lower priority policy it is *not allowed* to take effect.

Policies - Settings tab - Patch Reboot Action

Policy Management > Policies > Settings tab > Patch Reboot Action checkbox

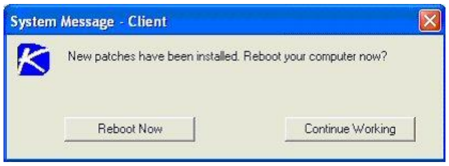
The **Patch Reboot Action** policy category assigns a **reboot action** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#358.htm)* to a policy for patch executable files.

- **Reboot immediately after update** - Reboots the computer immediately after the install completes.
- **Reboot <day of week> at <time of day> after install** - After the patch install completes, the computer is rebooted at the selected day of week and time of day. Use these settings to install patches during the day when users are logged in, then force a reboot in the middle of the night. Selecting **every day** reboots the machine at the next specified time of day following the patch installation.
- **Warn user that machine will reboot in <N> minutes (without asking permission)** - When the patch install completes, the message below pops open warning the user and giving them a specified number of minutes to finish up what they are doing and save their work. If no one is currently logged in, the system reboots immediately.



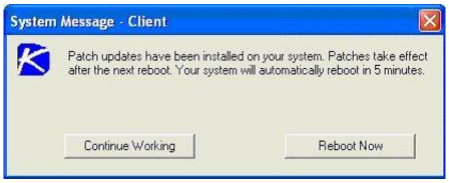
New updates have been installed on your system. Your system will automatically reboot in 5 minutes.

- **Skip reboot if user logged in** - If the user is logged in, the reboot is skipped after the patch install completes. Use this setting to avoid interrupting your users. This is the default setting.
- **If user logged in ask to reboot every <N> minutes until the reboot occurs** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears every N minutes repeatedly, until the system has been rebooted. If no one is currently logged in, the system reboots immediately.



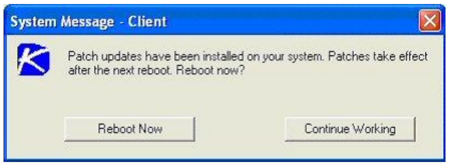
New patches have been installed. Reboot your computer now?

- **If user logged in ask permission. Reboot if no response in <N> minutes. Reboot if user not logged in** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, it reboots automatically after N minutes **without saving** any open documents. If no one is currently logged in, the system reboots immediately.

  Patch updates have been installed on your system. Patches take effect after the next reboot. Your system will automatically reboot in 5 minutes.

- **If user logged in ask permission. Do nothing if no response in <N> minutes. Reboot if user not logged in** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, the reboot is skipped. If no one is logged in, reboot immediately.

  Patch updates have been installed on your system. Patches take effect after the next reboot. Reboot now?

- **Do not reboot after update** - Does not reboot. Typically used if the machine is a server and you need to control the reboot. You can be notified via email when a new patch has been installed by checking **When reboot required, send email** and filling in an email address.

Policies - Settings tab - Patch Settings

Policy Management > Policies > Settings tab > Patch Settings checkbox

The **Patch Settings** category assigns patch settings to a policy.

Pre/Post Procedure *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2210.htm)*

Run procedures either before and/or after **Initial Update** or **Automatic Update**. For example, you can run procedures to automate the preparation and setup of newly added machines before or after **Initial Update**.

- **Run procedure before Initial Update**
- **Run procedure after Initial Update**
- **Run procedure before Automatic Update**
- **Run procedure after Automatic Update**

Patch Policy Membership *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#218.htm)*

Assign one or more patch policy names to this policy.

Patch Alert *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2889.htm)*

Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered.

- **Create Alarm**
- **Create Ticket**
- **Run Script** `<agentprocedure>` on `<machineID>`
- **Email Recipients** - Enter multiple addresses separated by commas.

> **Note:** This field may make use of **tokens** *(page 37)*.

The system can trigger an alert for the following alert conditions for a selected machine ID:

- **New patch is available**

- **Patch install fails**
- **Agent credential is invalid or missing**

> **Note:** An agent **credential** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* is not required to install patches **unless** the machine's File Source is configured as `Pulled from file server using UNC path`. If an agent credential is assigned, it will be validated as a local machine credential without regard to the **File Source** configuration. If this validation fails, the alert will be raised. If the machine's **File Source** is configured as `Pulled from file server using UNC path`, a credential is required. If it is missing, the alert will be raised. If it is not missing, it will be validated as a local machine credential and as a network credential. If either of these validations fails, the alert will be raised.

- **Windows Auto Update changed**

Policies - Settings tab - Patch Windows Automatic Update

Policy Management > Policies > Settings tab > Patch Windows Automatic Update checkbox

The **Patch Windows Automatic Update** category assigns the following policy:

- **Disable Windows Automatic Update to let Patch Management control system patching** - Check to disable **Windows Automatic Updates** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2070.htm)* on selected machine IDs and let **Patch Management** control patching of the managed machine. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user *cannot* change any of the settings. Users can still patch their systems manually.

Policies - Settings tab - Protection

Policy Management > Policies > Settings tab > Protection checkbox

The **Protection** category assigns file, application and network access to a policy.

File Access Control ***(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#405.htm)***

- **Add File** or **Change Access** - Adds and schedules **monitor sets** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#1938.htm)*. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered.
  - **Filename to access control (full path required)** - Enter the full path and file name.
  - **Enter application approved for access** - Add in a new application to the access list.
  - **Approved Applications** - Displays the list of applications approved for access.
  - **Remove** - Removes a selected application from the approved access list
  - **Ask user to approve unlisted** - Lets users approve/deny access to the file on a per application basis each time a new application tries to access that file. Use this feature to build up an access control list based on normal usage.
  - **Deny all unlisted** - Blocks an application from accessing the file. Select this option if you are already sure of which files need access and which do not.
- **Remove File** - Removes a selected agent procedure.

Application Blocker ***(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#409.htm)***

To block an application from running on a machine:

1. Enter the application's filename in the edit box.
2. Click the **Add** button. The blocked application displays in the **Application to block** list.

To unlbock an application from running on a machine:

1. Enter the application's filename in the edit box.
2. Click the **Remove** button. The application no longer displays in the **Application to block** list.

Network Access *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#407.htm)*

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

Policies - Settings tab - Remote Control

Policy Management > Policies > Settings tab > Remote Control checkbox

The **Remote Control** category assigns remote control **user notification** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2930.htm)* settings to a policy.

- **Select user notification type**:
  - **Silently take control -** Do not tell the user anything. Take control immediately and silently.
  - **If user logged in display alert** - Display notification alert text. The alert text can be edited in the text box below this option.
  - **If user logged in ask permission** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.
  - **Require Permission. Denied if no one logged in** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option.

Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. The remote control session is canceled.

- **Notify user when session terminates** - Notifies the user when the remote control session terminates.
- **Require admin note to start remote control** - Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.

Policies - Settings tab - Software Deployment Profile Assignment

Policy Management > Policies > Settings tab > Software Deployment Profile Assignment checkbox

The **Software Deployment Profile Assignment** category assigns a **Software Deployment and Update** profile and schedule pattern to a policy. Machines assigned this policy must be installed with **Software Deployment and Update**.

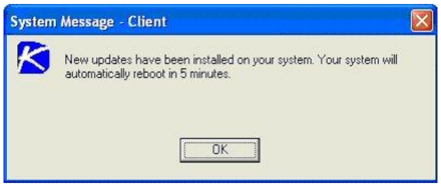
- **Deployment Pattern** - The recurring deployment schedule. Schedule patterns are configured using the Software Deployment and Update > **Application Settings** *(http://help.kaseya.com/webhelp/EN/KSDU/9040000/index.asp#9819.htm)* > **Schedule Patterns** tab.
- **Add Profile** - Adds a **Software Deployment and Update profile** *(http://help.kaseya.com/webhelp/EN/KSDU/9040000/index.asp#9815.htm)* to this policy.
- **Remove Profile** - Removes a profile from this policy.

Policies - Settings tab - Software Deployment Reboot Action

Policy Management > Policies > Settings tab > Software Deployment Reboot Action checkbox

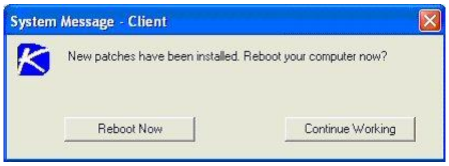
The **Software Deployment Reboot Action** policy category assigns a **Software Deployment and Update reboot action** *(http://help.kaseya.com/webhelp/EN/KSDU/9040000/index.asp#9821.htm)* to a policy. Machines assigned this policy must be installed with **Software Deployment and Update**.

- **Reboot immediately after update** - Reboots the computer immediately after the install completes.
- **Reboot <day of week> at <time of day> after install** - After the patch install completes, the computer is rebooted at the selected day of week and time of day. Use these settings to install patches during the day when users are logged in, then force a reboot in the middle of the night. Selecting **every day** reboots the machine at the next specified time of day following the patch installation.
- **Warn user that machine will reboot in <N> minutes (without asking permission)** - When the patch install completes, the message below pops open warning the user and giving them a specified number of minutes to finish up what they are doing and save their work. If no one is currently logged in, the system reboots immediately.



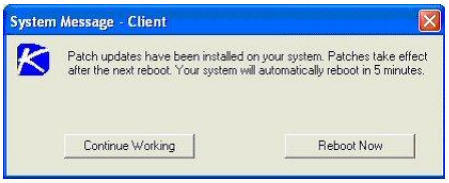
New updates have been installed on your system. Your system will automatically reboot in 5 minutes.

- **Skip reboot if user logged in** - If the user is logged in, the reboot is skipped after the patch install completes. Use this setting to avoid interrupting your users. This is the default setting.
- **If user logged in ask to reboot every <N> minutes until the reboot occurs** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears every N minutes repeatedly, until the system has been rebooted. If no one is currently logged in, the system reboots immediately.



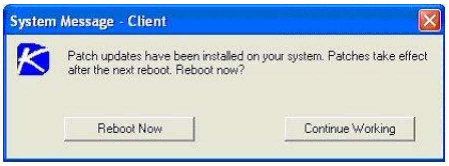
New patches have been installed. Reboot your computer now?

- **If user logged in ask permission. Reboot if no response in <N> minutes. Reboot if user not logged in** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, it reboots automatically after N minutes **without saving** any open documents. If no one is currently logged in, the system reboots immediately.



Patch updates have been installed on your system. Patches take effect after the next reboot. Your system will automatically reboot in 5 minutes.

- **If user logged in ask permission. Do nothing if no response in <N> minutes. Reboot if user not logged in** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, the reboot is skipped. If no one is logged in, reboot immediately.



Patch updates have been installed on your system. Patches take effect after the next reboot. Reboot now?

- **Do not reboot after update** - Does not reboot. Typically used if the machine is a server and you need to control the reboot. You can be notified via email when a new patch has been installed by checking **When reboot required, send email** and filling in an email address.

Policies - Settings tab - Software Deployment Scan Schedule

Policy Management > Policies > Settings tab > Software Deployment Scan Schedule checkbox

The **Software Deployment Scan Schedule** category assigns a **Software Deployment and Update** scan schedule to a policy. Machines assigned this policy must be installed with **Software Deployment and Update**. Schedule patterns are configured using the Software Deployment and Update > **Application Settings** *(http://help.kaseya.com/webhelp/EN/KSDU/9040000/index.asp#9819.htm)* > **Schedule Patterns** tab.

- **Baseline Scan** - The recurring baseline scan schedule.
- **Lastest Scan** - The recurring latest scan schedule.

Policies - Settings tab - Suspend Alarms

Policy Management > Policies > Settings tab > Suspend Alarms checkbox

The **Suspend Alarms** category assigns a **suspend alarm** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2185.htm)* schedule to a policy. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms.*

- **Add Suspend Schedule** - Configures suspending alarms once or for a recurring period.
  - **Suspend alarms at <date> <time>** - Specify the start date and start time.
  - **recurring every <N> periods** - Enter 0 or leave blank to suspend alarms once.
  - **Suspend alarms for <N> periods** - Set the duration that alarms are suspended.
- **Remove Suspend Schedule**

Policies - Settings tab - Update List by Scan

Policy Management > Policies > Settings tab > Update List by Scan checkbox

The **Update List by Scan** category assigns **Update List by Scan** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#1948.htm)* schedules to a policy.

For Windows 2000 and Earlier Windows Machines - Users may elect to run **Update Lists by Scan** on a recurring basis for the purpose of discovering new counter objects on those machines. This is the only reason to run **Update Lists by Scan** on a recurring basis.

- **Edit Schedule** - Edits an existing scan schedule. Schedule a task once or periodically. Each type of recurrence—Once, Minutes, Hourly, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. Options can include:
  - **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.
  - **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. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
  - **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. Applies only to recurring schedules, a 'Once' schedule always executes the next time the agent is online.
  - **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-network or vPro and another managed system on the same network.
  - **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.
- **Reset** - A schedule for this type of scan is not set for this policy. If this same type of scan has a schedule defined in a lower priority policy it is *allowed* to take effect.
- **None** - A schedule for this type of scan is not set for this policy. If this same type of scan has a schedule defined in a lower priority policy it is *not allowed* to take effect.

Policies - Settings tab - Working Directory

Policy Management > Policies > Settings tab > Working Directory checkbox

The **Work Directory** category assigns a **working directory** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#368.htm)* to a policy.

- **Working Directory** - Sets the path to a directory on the managed machine used by the agent to store working files.

Settings

Policy Management > Settings

The **Settings** page schedules the interval for automatic deployment of all policies to all assigned machines.

Deployment Interval

This setting determines how frequently policy deployment occurs. Policies may be associated with machines, machine groups or organizations. As new machines appear or their existing associations are changed, policies may need to be deployed or re-deployed. Setting the deployment interval to manual requires the user to click the **Apply Now** button on the **Policies** *(page 5)* page to deploy a policy.

> **Note: Policy Management** has a recurring process that automatically detects view membership changes for all agent machines. This is a very intensive process. As such, the schedule for this process is not tied to the **Deployment Interval**. Instead, the view membership process runs once per hour on a schedule that is set by the system. In those cases where you want view membership to be re-evaluated immediately you can use the **Machines** *(page 28)* > **Reprocess Policies** button for one or more selected machines.

Edit Schedule

A compliance check compares an agent settings with the policies assigned that agent to determine if it is in compliance. For policies that require a credential be set, **Policy Management** now sets a policy object status as out of compliance when the policy fails to be processed due to an unsupported operating system or invalid agent credentials.

Click **Edit Schedule** to display the **Schedule Compliance Check** window. Each type of recurrence—Once, Minutes, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:

- **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.
- **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. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
- **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. Applies only to recurring schedules, a 'Once' schedule always executes the next time the agent is online.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-network or vPro and another managed system on the same network.
- **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.

Reset

- Removes the scheduled compliance check.

Organizations / Machine Groups

Policy Management > Organizations / Machine Groups

The **Organizations / Machine Groups** page assigns policies to organizations and machine groups. A **System cabinet** *(page 36)* provides built-in policies that reflect best-practice solutions for common IT management tasks. Policies can be configured for an organization automatically using the **Systems Management Configuration setup wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9040000/index.asp#11220.htm)* and these System cabinet policies.

Actions

- **Remove** - Removes a selected policy from an organization or machine group.
- **Select & Assign** - Selects and assigns a policy to an organization or machine group. This button only enables if a view is assigned the selected policy, and both the policy and at least one organization or machine group is selected.
- **Select All** - Selects all organizations.
- **Unselect All** - Unselects all organizations.
- **Collapse All** - Fully collapses the organization/machine group tree.
- **Expand All** - Fully expands the organization/machine group tree.
- **Remind me that items will automatically synchronize when moved** - If checked, displays a popup warning message that changes will be applied immediately. Applies to each VSA user individually.
- **(Folder Tree Filters)** - Applies to **Machine Groups** cabinet and **Policies** cabinet and System cabinet - Enter text in the filter edit box, then click the funnel icon to apply filtering to the folder tree. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder tree.

Assigning Policies

Drag and drop a policy from the **Policies** folder tree in the right hand pane to the **Machine Groups** tree in the middle pane.

Policies Without Views

Assigning a policy to a view on the Policies page is *required* to assign a policy using the **Organizations/Machine Groups** *(page 26)* page. *This prevents the unintentional assignment of a policy to all machines in the VSA.* A policy without a specified view displays as a red scroll icon in the policy tree of the **Organizations/Machine Groups** page, indicating that it cannot be assigned. A folder with a red exclamation mark icon displays in the policy tree if it contains at least one policy without a specified view. When assigning an entire folder of policies to an organization or machine group, policies without a specified view are ignored.

Policies Assignment Rules

- Multiple policies can be assigned to any organization or machine group or machine.
- A machine with multiple policies assigned to it has **conflicting policies** when both specify the *same* policy type.
  - Multiple policies are not in conflict if different policy types are specified.
  - Policy types that **combine with each other** include:
    - ✓ Event log alerts, distribute files, monitor sets, and agent procedures.
- Policies are assigned *by organization/machine group* using the **Organizations/Machine Groups** *(page 27)* page.
  - Policies assigned to a child node in an organization hierarchy have precedence over policies assigned to a parent node in the same organization hierarchy.
  - Unless a child node policy conflicts with it, policies assigned to a node apply to all descendant nodes.

    - When multiple policies are assigned to the same organization or machine group, the assigned policies have precedence in the order listed.
- Policies can be assigned *by machine* using the **Machines** *(page 28)* page.
    - Policies assigned *by machine* have precedence over all policies assigned to that machine *by organization/machine group*.
    - Policies assigned by machine have precedence in the order listed.
- All policy assignments can be *overridden* by changing agent settings *manually* throughout the VSA.
    - Manual changes have precedence over all policies assignments.
- A policy can be associated with a *view definition* in the **Policies** *(page 5)* page.
    - When machine is assigned to a policy *by organization* or by *machine group* an associated view *filters* the machines associated with a policy. If a machine is not a member of the view definition, then the policy will not be propagated to that machine.
    - When a machine is assigned to a policy *by machine*, then the view associated with a policy is ignored and the policy will be propagated to that machine.
    - Associating a policy with a view does *not, by itself*, assign a policy to any machine.
- The order of precedence for views depends on the policies they are associated with.

Machines

Policy Management > Machines

The **Machines** page assigns policies to individual machines. The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using.

Machine Compliance Status

The middle pane shows the policy compliance status for each machine, in the following order of precedence.

- `In Compliance` - The agent settings for this machine match the settings of all policies assigned to this machine.

- `Out of Compliance` - At least one agent setting does not match at least one active policy assigned to this machine.

- `Marked for Deployment` - At least one policy assigned to this machine has been changed and is scheduled to be deployed.

- `Overridden` - At least one agent setting does not match at least one active policy assigned to this machine, *due to a user override*. An override occurs when an agent setting is set manually by any VSA user anywhere in the system. If even a single agent setting is overridden in a policy assigned to a machine, no other agent settings in that policy are enforced on that machine. Other policies assigned to the same machine remain enforced.

Note: Click the policy status icon to display the **Policy Matrix** *(page 4)* > **Matrix Details** window for that machine.

Actions

- **Assign** - Assigns policies to selected machines.
- **Clear Override** - Clears **Policy Management** policy overrides on selected machines. *After clicking* **Clear Override**, *the user must click* **Reprocess Policies** *to ensure the policy objects that were overridden before are reapplied to the agent.* A **Policy Management** policy override condition exists if agent settings for a machine have been set manually, outside of the **Policy Management**

module. For example, making changes to the agent menu of a machine using the **Agent Menu** page in the **Agent** module sets up an override condition for that agent machine. **Policy Management** policies will be ignored from then on. Clearing an override enables applied **Policy Management** policies to take effect.

- **Reprocess Policies** - All policy objects assigned to a machine can be re-marked for deployment and reprocessed as though they were assigned to that machine for the first time. To reduce unnecessary server activity and network traffic, each policy object is deployed only *once* to a machine, even if additional policies are assigned to that machine that include the same policy object. If agent settings for a machine are unexpected, use this option to re-deploy all policy objects assigned to a machine.

Right Hand Pane

The right hand pane is divided into two horizontal sections.

- **Policies Assigned to this Machine** - Displays policies assigned by machine.
- **Policies Assigned to this Machine by Association with Organizations/Machine Groups** - Displays policies assigned by organization and machine group.

Actions

- **Move Up** and **Move Down** - You can re-order the sequence of policies assigned to the machine.
- **Remove** - You can remove policies assigned to the machine.

Policy Assignment Rules

- Multiple policies can be assigned to any organization or machine group or machine.
- A machine with multiple policies assigned to it has **conflicting policies** when both specify the *same* policy type.
  - ➢ Multiple policies are not in conflict if different policy types are specified.
  - ➢ Policy types that **combine with each other** include:
    - ✓ Event log alerts, distribute files, monitor sets, and agent procedures.
- Policies are assigned *by organization/machine group* using the **Organizations/Machine Groups** *(page 27)* page.
  - ➢ Policies assigned to a child node in an organization hierarchy have precedence over policies assigned to a parent node in the same organization hierarchy.
  - ➢ Unless a child node policy conflicts with it, policies assigned to a node apply to all descendant nodes.
  - ➢ When multiple policies are assigned to the same organization or machine group, the assigned policies have precedence in the order listed.
- Policies can be assigned *by machine* using the **Machines** *(page 28)* page.
  - ➢ Policies assigned *by machine* have precedence over all policies assigned to that machine *by organization/machine group*.
  - ➢ Policies assigned by machine have precedence in the order listed.
- All policy assignments can be *overridden* by changing agent settings *manually* throughout the VSA.
  - ➢ Manual changes have precedence over all policies assignments.
- A policy can be associated with a *view definition* in the **Policies** *(page 5)* page.
  - ➢ When machine is assigned to a policy *by organization* or by *machine group* an associated view *filters* the machines associated with a policy. If a machine is not a member of the view definition, then the policy will not be propagated to that machine.
  - ➢ When a machine is assigned to a policy *by machine*, then the view associated with a policy is ignored and the policy will be propagated to that machine.
  - ➢ Associating a policy with a view does *not, by itself*, assign a policy to any machine.

- The order of precedence for views depends on the policies they are associated with.

Policy Management - Agents Policy Status

Info Center > Reporting > Reports > Policy Management - Agent Policy Status

- Displays only if the Policy Management add-on module is installed.

The **Agents Policy Status** report definition generates a policy status report. Can be filtered by:

- **Agent's Policy Status**
- **Policy Object Type**
- **Policy Object Status**

Policy Management - Policy Info & Association

Info Center > Reporting > Reports > Policy Management - Policy Info & Association

- Displays only if the Policy Management add-on module is installed.

The **Policy Info & Association** report definition generates a report of policies and associations. Can be filtered by:

- **Policy Status**
- **Policy Object Type**

Copyright 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 Kseya 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."

Glossary

Credentials

A credential is a username and password used to authenticate a user or process's access to a machine or network or some other resource.

Agent Credentials

The VSA maintains a single *agent credential* with administrator privileges for an agent to use, using the Agent > Manage Agents page.

- Patch Management - If an agent credential is defined for a machine ID, then Patch Management installs all new patches using this agent credential. Therefore, the agent credential should always be a user with administrator rights.
- Patch Status - Patch Status resets test results every time a machine ID's agent credential changes.
- File Source - File Source may require an agent credential be defined for the machine ID acting as the file share.
- Patch Alert - Set up an alert to notify you if a machine ID's agent credential is missing or invalid.
- Office Source - A machine ID must have an agent credential to access the alternate Office source location, in case a patch is being installed when no user is logged into the machine.
- If-Then-Else - The `useCredential()` command in the agent procedure editor requires a an agent credential to run successfully.
- **Backup** > **Image Location** *(http://help.kaseya.com/webhelp/EN/KSD/9040000/index.asp#7948.htm)* - If a UNC path is specified in **Image Location**, an agent credential must be defined to provide access to this UNC path. Without the agent credential, the machine will *not* have access to the image location and the backup will fail. When specifying a UNC path to a share accessed by an agent machine—for example \\machinename\share—ensure the share's permissions allow read/write access using the agent credential.
- View Definitions - Includes a **Machines with Credential status** option that allows you to filter the display of machine IDs on any agent page by their agent credential status.
- Desktop Management - Installing the client for this module requires an agent credential be defined.

Blank Credentials

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

Managed Credentials

The VSA maintaines *additional* credentials at three different levels: by organization, by machine group and by individual machine or device. They are managed using three navigation items in the **Audit** module:

- View Assets - Use this page to create multiple credentials for an *individual* machine or device.
- Manage Credentials - Use this page to create multiple credentials for *organizations* and *machine groups* within organizations.
- Credential Log - This page logs the creation, display and deletion of managed credentials.

Once created, use managed credentials:

- To instantly lookup all the credentials that apply to a machine you're working on. The Quick View (Classic) popup window includes a **View Credentials** option. Access is controlled by role and by scope. You can add a description for each credential.
- As the *source credential* for an agent credential in a policy. Check the **Use organization defaults** checkbox in the **Credential** setting of the Policy Management > Policies page to establish the link.

> **Note:** A managed credential can not overwrite the agent credential maintained using the Agent > Manage Agents directly. The managed credential must be applied to a policy and the policy applied to the machine.

If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the *source credential* for an agent credential for Policy Management

myOrg

`myOrg` is the **organization** *(page 34)* of the service provider using the VSA. All other organizations in the VSA are second party organizations doing business with `myOrg`. The default name of `myOrg`, called `My Organization`, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the* `myOrg` *organization.* `myOrg` cannot be assigned a parent organization.

On Premises

An **on premises** hardware/software installation of the VSA is a maintained by a service provider and typically used only by the service provider. See **Software as a Service (SaaS)** *(page 36)*.

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 **Service Billing**.
- **Vendors** - Supports the procurement of materials using **Service Billing**.

The `Org` table is a support table shared by *organizations*, *customers* and *vendors*. Each record in the `Org` table is identified by a unique `orgID`. The `Org` table contains basic information you'd generally need to maintain about any kind of business relationship: mailing address, primary phone number, duns number, yearly revenue, etc. Because the `Org` table is shared, you can easily convert:

- A customer into an organization or vendor.
- A vendor into an organization or customer.
- An organization into a customer or vendor.

> **Note:** `myOrg` (page 34) is the organization of the service provider using the VSA.

Patch Policy

Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.

- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- Initial Update and Automatic Update require patches be approved before these patches are installed.
- Approval by Policy approves or denies patch by *policy*.
- Approval by Patch approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- KB Override overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- Patch Update and Machine Update can install denied patches.
- Non-`Master` role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

Policies and Views

Assigning a policy to a view on the Policies page is *required* to assign a policy using the **Organizations/Machine Groups** *(page 26)* page. *This prevents the unintentional assignment of a policy to all machines in the VSA.* A policy without a specified view displays as a red scroll icon in the policy tree of the **Organizations/Machine Groups** page, indicating that it cannot be assigned. A folder with a red exclamation mark icon displays in the policy tree if it contains at least one policy without a specified view. When assigning an entire folder of policies to an organization or machine group, policies without a specified view are ignored.

Policy Assignment Rules

- Multiple policies can be assigned to any organization or machine group or machine.
- A machine with multiple policies assigned to it has **conflicting policies** when both specify the *same* policy type.
  - Multiple policies are not in conflict if different policy types are specified.
  - Policy types that **combine with each other** include:
    - Event log alerts, distribute files, monitor sets, and agent procedures.
- Policies are assigned *by organization/machine group* using the **Organizations/Machine Groups** *(page 27)* page.
  - Policies assigned to a child node in an organization hierarchy have precedence over policies assigned to a parent node in the same organization hierarchy.
  - Unless a child node policy conflicts with it, policies assigned to a node apply to all descendant nodes.
  - When multiple policies are assigned to the same organization or machine group, the assigned policies have precedence in the order listed.
- Policies can be assigned *by machine* using the **Machines** *(page 28)* page.
  - Policies assigned *by machine* have precedence over all policies assigned to that machine *by organization/machine group*.
  - Policies assigned by machine have precedence in the order listed.
- All policy assignments can be *overridden* by changing agent settings *manually* throughout the VSA.
  - Manual changes have precedence over all policies assignments.
- A policy can be associated with a *view definition* in the **Policies** *(page 5)* page.

- When machine is assigned to a policy *by organization* or by *machine group* an associated view *filters* the machines associated with a policy. If a machine is not a member of the view definition, then the policy will not be propagated to that machine.
- When a machine is assigned to a policy *by machine*, then the view associated with a policy is ignored and the policy will be propagated to that machine.
- Associating a policy with a view does *not, by itself*, assign a policy to any machine.
- The order of precedence for views depends on the policies they are associated with.

Policy Overrides

A **Policy Management** policy override condition exists if agent settings for a machine have been set manually, outside of the **Policy Management** module. For example, making changes to the agent menu of a machine using the **Agent Menu** page in the **Agent** module sets up an override condition for that agent machine. **Policy Management** policies will be ignored from then on. Clearing an override enables applied **Policy Management** policies to take effect.

Policy Status Icons

- `In Compliance` - The agent settings for this machine match the settings of all policies assigned to this machine. No user action is required.

- `Marked for Deployment` - At least one policy assigned to this machine has been changed and is scheduled to be deployed. No user action is required.

- `No Policy Attached` - No *applied* policies are assigned to this machine. Consider assigning *applied* policies to this machine.

- `Out of Compliance` - At least one agent setting does not match at least one active policy assigned to this machine. Use the **Policy Details** window to identify the specific policies and settings that are causing the mismatch.

- `Overridden` - At least one agent setting does not match at least one active policy assigned to this machine, *due to a user override*. An override occurs when an agent setting is set manually by any VSA user anywhere in the system. Use the **Policy Details** window to confirm the override of specific policies and settings are correct. If even an single agent setting is overridden in a policy assigned to a machine, no other agent settings in that policy are enforced on that machine. Other policies assigned to the same machine remain enforced.

- `Inactive` - *This policy status only displays in the* **Policy Details** *window.* When multiple policies are assigned to a machine and agent settings conflict, **policy assignment rules** *(page 27)* determine which agent settings are obeyed and which agent settings are ignored. Ignored settings are identified as inactive. A machine can show an `In Compliance` policy status icon while the *Policy Details* windows shows specific agent settings in specific policies as `Inactive`. This is expected behavior. No user action is required.

Software as a Service (SaaS)

Sharing the capabilities of a single instance of the VSA is oftentimes called "Software as a Service". Service providers contract to access a VSA hosted and maintained by a VSA *tenant manager*. Service providers are allocated a unique *tenant partition* of a shared Kaseya Server and database. Within their assigned partition, service providers can only see their own organizations, machine groups, agents, procedures, reports, tickets, and any other types of user-defined data. Service providers in a tenant partition have full access to most functions of the VSA except system maintenance, which is the responsibility of the VSA tenant manager.

System Cabinets

Built-in data objects are provided with the VSA and addon modules. These built-in data objects—also called *content*—provide users with best-practice solutions for commonly required IT management tasks. In some cases these built-in data objects are organized by *System cabinet* in a data object tree. Examples include:

- Policies - Policy Management > Policies
- Agent Procedures - Agent Procedures > Create / Schedule
- Monitor Sets - Monitor > Monitor Sets

You cannot modify a system cabinet policy. To copy a policy, hold down the CTRL key and drag the policy from one folder to another.

Tokens

To enable multiple organizations to make use of the same built-in, standard policies in **Policy Management**, placeholder **tokens** are entered in policy fields requiring an email address. These token values are `#patchAlertEmail#`, `#sev1AlertEmail#`, `#sev2AlertEmail#`, and `#sev3AlertEmail#`. The VSA automatically replaces a token in a policy with the appropriate email address for a specific organization when an alert notification is sent out. The organization email addresses referenced by tokens are specified using step 1 of the **System Management Configure Wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9040000/index.asp#11221.htm)*. This wizard can be run during setup or anytime afterwards from the System > Orgs/Groups/Depts/Staff > Manage > **Systems Management tab** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#11372.htm)*. The **Policy Management** policy categories that include email addresses are **Alerts** *(page 9)*, **Monitor Sets** *(page 16)* and **Patch Settings** *(page 20)*.

Index