Kaseya 2

Policy Management

User Guide

Version 1.0

June 6, 2012

About Kaseya

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

Contents

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 KPM policy override condition exists if agent settings for a machine have been set manually, outside of the KPM 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. KPM 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-Online-Help.asp?6963.htm)*.

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 17)* 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 17)* page.
2. Define agent setting policies using the **Policies** *(page 4)* page.
3. Apply policies to:
   - Organizations and machine groups using the **Organizations / Machine Groups** *(page 18)* page.
   - Individual machines using the **Machines** *(page 19)* page. You can also clear KPM 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 3)* page and **Dashboard** *(page 3)* page.
5. Monitor **Policy Management** activity using the **Logs** *(page 3)* page.

Note: See **KPM System Requirements** *(page 2)*.

Functions	Description
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 3)*	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 4)*	Defines agent settings by policy, including • Agent Menu • Agent Procedure • Alerts • Check-in • Credential • Distribute File - This policy object is not available in a SaaS-based VSA. • Logging • Machine Profile • Monitor Sets • Patch Settings • Protection • Remote Control • Working Directory
Settings *(page 17)*	Schedules the interval for automatic deployment of all policies to all assigned machines.
Organizations / Machine Groups *(page 18)*	Assigns policies to organizations and machine groups.
Machines *(page 19)*	Assigns policies to individual machines.

Policy Management System Requirements

Kaseya Server

- The **Policy Management** module installs on VSA 6.1 or later

> **Note:** See general **System Requirements** *(http://help.kaseya.com/WebHelp/EN/System-Requirements.asp).*

Dashboard

Policy Management > Dashboard

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

- **Policy Status** - Hover the cursor over a pie slice to see the amount and percentage that pie slice represents.
- **Agent Policy Status** - Hover the cursor over a pie slice to see the amount and percentage that pie slice represents.
- **Pending Events** - Lists policies that have been changed and saved, but not yet applied. *Only applied settings are propagated to assigned machines.*

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-Online-Help.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 each policy assigned to a machine ID.

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 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 18)* 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.

Policy Status Icons

Policies may be active or inactive, depending on their order or precedence, whether they have been overridden, or are out of compliance. You can filter the page by selecting `Active`, `Inactive`, or `All` policies.

Policies

Policy Management > Policies

The **Policies** page defines agent policies. Policies are organized by a **folder tree** *(page 5)*. A selected policy displays three tabs in the right hand pane:

- **Settings** *(page 5)* - 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 18)* 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 18)* page.
  - The individual machines assigned this policy using the **Machines** *(page 19)* page.
  - The view associated with this policy using the **Settings** *(page 5)* tab of the **Policies** page. A view associated with a policy filters machine membership in that policy.

> **Note:** The view associated with a policy is ignored if the policy is assigned *by machine* using the **Machines** page.

- 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**.
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 17)* page.

Policies - Folder Tree

Policy Management > Policies > Folder Tree

Policies are organized using a folder tree of *organizations and machine groups* 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 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.

When a Folder or Policy is Selected

- **Rename Folder** - Renames a selected folder.
- **Delete Folder** - Deletes a selected folder.
- **Apply All Policies** - Applies all policy changes to a selected policy.

Policies - Settings tab

Policy Management > Policies > Settings tab

Agent policy settings are grouped by setting category in this tab. Click a setting 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 17)* 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 17)* 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 scroll 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 19)* page.

Setting Categories

- **Policies - Settings tab - Agent Menu** *(page 6)*
- **Policies - Settings tab - Agent Procedure** *(page 7)*
- **Policies - Settings tab - Alerts** *(page 7)*
- **Policies - Settings tab - Check-in** *(page 8)*
- **Policies - Settings tab - Credential** *(page 9)*
- **Policies - Settings tab - Distribute File** *(page 10)* - This policy object is not available in a SaaS-based VSA.
- **Policies - Settings tab - Log History** *(page 10)*
- **Policies - Settings tab - Machine Profile** *(page 11)*
- **Policies - Settings tab - Monitor Sets** *(page 12)*
- **Policies - Settings tab - Patch Settings** *(page 12)*
- **Policies - Settings tab - Protection** *(page 15)*
- **Policies - Settings tab - Remote Control** *(page 16)*
- **Policies - Settings tab - Working Directory** *(page 17)*

Policies - Settings tab - Agent Menu

Policy Management > Policies > Settings tab > Agent Menu checkbox

Agent Menu

- **Enable Agent Icon** - Check to display the agent icon in the system tray of the managed machine. Uncheck to hide the agent icon and prevent the use of agent menu options.
- **About <Agent>** - Check to enable the machine user to click this option to display the About box for the installed agent. The default option label `Agent` can be customized.

- **<Contact Administrator...>** - Check to enable the machine user to click this option to display either the user's Portal Access page or a different contact URL. The default option label `Contact Adminitrator...` can be customized.
- **<Your Company URL...>** - Check to enable the machine user to click this option to display the URL specified in the corresponding URL field.
- **Disable Remote Control** - Check to enable the machine user click this option to *disable* remote control on the user's managed machine.
- **Set Account...** - Check to enable the machine user to click this option to display their machine ID.group ID.organization ID and change the Kaseya Server address the agent checks into.
- **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 Procedure

Policy Management > Policies > Settings tab > Agent Procedure checkbox

Agent Procedures

- **Add Procedure** - Adds and schedules an **agent procedure** *(http://help.kaseya.com/WebHelp/EN/VSA-Online-Help.asp?2845.htm)*.
- **Remove Procedure** - Removes a selected agent procedure.

Policies - Settings tab - Alerts

Policy Management > Policies > Settings tab > Alerts checkbox

Alerts

- **Add Alert**
  - The **Alerts - Agent Status** page triggers an alert when an agent is offline, first goes online, or someone has disabled remote control on the selected machine.
  - The **Alerts Application Changes** page triggers an alert when a new application is installed or removed on selected machines.
  - The **Alerts - Get File** page triggers an alert 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 not a previous copy on the Kaseya Server, the alarm condition is encountered.
  - The **Alerts - Hardware Changes** page triggers an alert 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 triggers an alert when available disk space falls below a specified percentage of free disk space.
  - The **Event Log Alerts** page triggers an alert when an event log entry for a selected machine matches a specified criteria. After selecting the **event log type**, you can filter the alarm conditions specified by **event set** and by **event category**.
  - The **Alerts - LAN Watch** page works in conjunction with **LAN Watch** *(http://help.kaseya.com/WebHelp/EN/KDIS-Online-Help.asp?1944.htm)* pages. **LAN Watch** scans a machine ID's local LAN and detects new machines and devices connected to the machine's LAN. Both **LAN Watch** and the **Alerts - LAN Watch** page can subsequently trigger an alert when a new machine or device is discovered on a LAN. Only the **Alerts - LAN Watch** page can create a ticket when a new machine or device is discovered on a LAN.

- The **Alerts - Agent Procedure Failure** page triggers an alert when an agent procedure fails to execute on a managed machine.
- The **Alerts - Protection Violation** page triggers an alert when a file is changed or access violation detected on a managed machine.
- The **Alerts - Patch Alert** page triggers an alert for patch management events on managed machines.

- **Remove Alert** - Removes a selected alert.

Policies - Settings tab - Check-in

Policy Management > Policies > Settings tab > Check-in checkbox

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 page. A lock icon in the paging areas shows the agent is bound. To *unbind* agents, select machines IDs, ensure **Bind to Kserver** is unchecked and click **Update**. The lock icon no longer displays for selected machines.

Bandwidth Throttle

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

Warn if multiple agents use same account

The 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

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 File

Policy Management > Policies > Settings tab > Distribute File checkbox

> **Note:** The **Distribute File** policy object in is not available in a SaaS-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 - Log History

Policy Management > Policies > Settings tab > Log History checkbox

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 alarm conditions that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **Sys Log** - The log of all System Check external systems.

Set days to keep monitoring logs for all machines

The following monitoring log settings are applied system-wide.

- **Event Log** - The log of all events. The events collected are specified in more detail using Agent > Event Log Settings.
- **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

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 Proflle** 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 this checkbox checked.

Policies - Settings tab - Monitor Sets

Policy Management > Policies > Settings tab > Monitor Sets checkbox

Monitor Sets

- **Add Monitor Set** - Adds and schedules **monitor sets** *(http://help.kaseya.com/WebHelp/EN/VSA-Online-Help.asp?1938.htm)*. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered.
  - **Create Alarm**
  - **Create Ticket**
  - **Run Script** `<agentprocedure>` on `<machineID>`
  - **Email Recipients** - Enter multiple addresses separated by commas.
- **Remove Monitor Set** - Removes a selected agent procedure.

Policies - Settings tab - Patch Settings

Policy Management > Policies > Settings tab > Patch Settings checkbox

Pre/Post Procedure

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**.

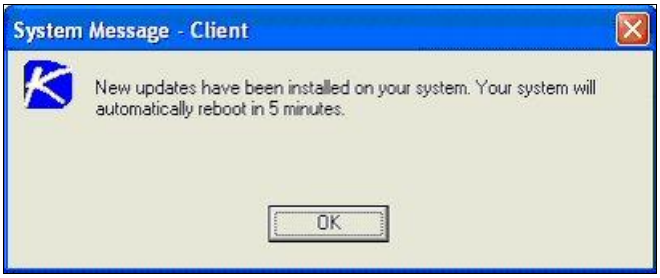
- **Run procedure before Initial Update**
- **Run procedure after Initial Update**
- **Run procedure before Automatic Update**
- **Run procedure after Automatic Update**

Patch Policy Membership

Assign one or more patch policy names to this policy.

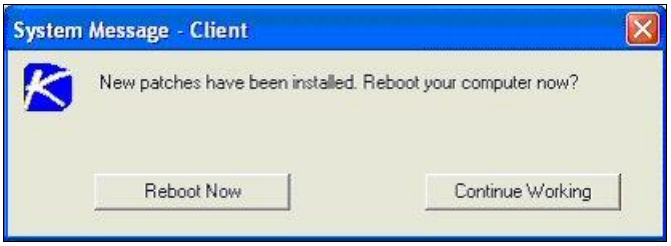
Reboot Action

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

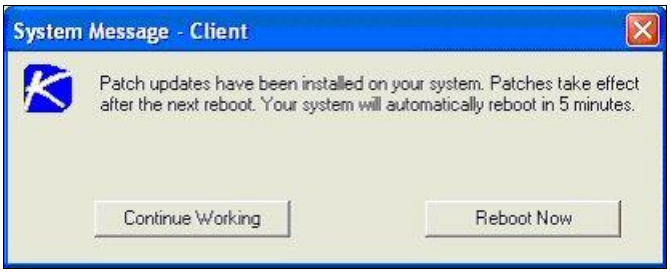


- **Skip reboot if user logged in** - If the user is logged in, the reboot is skipped after the patch install completes. Use this setting to avoid interrupting your users. This is the default setting.

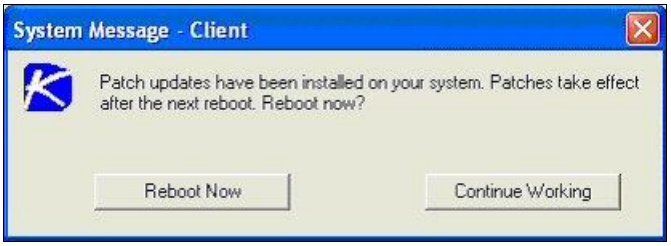
- **If user logged in ask to reboot every <N> minutes until the reboot occurs** - This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears every N minutes repeatedly, until the system has been rebooted. If no one is currently logged in, the system reboots immediately.



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



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



- **Do not reboot after update** - Does not reboot. Typically used if the machine is a server and you need to control the reboot. You can be notified via email when a new patch has been installed by checking **Email when reboot required** and filling in an email address. You can also format the email message by clicking the **Format Email** button. This option only displays for master role users.

The following types of patch reboot emails can formatted:

- Patch Reboot

> **Note:** *Changing the email alarm format changes the format for all* **Patch Reboot** *emails.*

The following variables can be included in your formatted email alerts and in procedures.

- `<at>` - alert time
- `<db-view.column>` - Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
- `<gr>` - group ID
- `<id>` - machine ID

- **Run select agent procedure before machine is rebooted** - If checked, the selected agent procedure is run just *before* the machine is rebooted.

Run select agent procedure after machine is rebooted - If checked, the selected agent procedure is run just *after* the machine is rebooted.

File Source

- **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. A **Clear Cache** button displays for this option only in Patch Management > File Source. Click **Clear Cache** to clear all downloaded patches stored on 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 the local directory of a selected machine ID. The local directory on the machine ID is configured to be shared with other machine IDs on the same LAN. All other machine IDs on the same LAN use a UNC path to the shared folder located on the first machine ID. All other machines on the same LAN require a credential to access the shared folder on the first machine and install the patch files. A credential is specified for the first machine with the shared directory using Agent > Set Credential.

Setup

1. Enter a UNC path in the **Pulled from file server using UNC path** field. For example, `\\computername\sharedname\dir\`.
2. Use the **Machine Group Filter** drop-down list to select a group ID.
3. Select a machine ID from the **File share located on** drop-down list.
4. Enter a shared local directory in the **in local directory** field.

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

   First the Kaseya Server checks to see if the patch file is already in the file share. If not, the machine ID with the file share automatically loads the patch file either directly from the internet or gets it from the Kaseya Server. In either case, the managed machine with the file share **must have an agent** on it.
5. **File Server automatically gets patch files from** - Select one of the following options:
   - **the Internet** - Use this setting when the managed machine running the file share has full internet access.

- **the system server** - Use this setting when the managed machine running the file share is blocked from getting internet access.

6. **Download from Internet if machine is unable to connect to the file server** - Optionally check this box to download from the internet. This is especially useful for laptops that are disconnected from the company network but have internet access.

Patch Alert

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

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

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

- **New patch is available**
- **Patch install fails**
- **Agent credential is invalid or missing**

> **Note:** An agent credential 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**

Patch Procedures Schedule

- **Patch Scan** - 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. Schedule and clear the schedule using **Edit Schedule** and **Reset**.
- **Automatic Update** - Schedules an update of managed machines with Microsoft patches on a *recurring* basis. **Automatic Update** obeys both the Patch Approval Policy and the Reboot Action policy. Schedule and clear the schedule using **Edit Schedule** and **Reset**.

Policies - Settings tab - Protection

Policy Management > Policies > Settings tab > Protection checkbox

File Access Control

- **Add File** or **Change Access** - Adds and schedules **monitor sets** *(http://help.kaseya.com/WebHelp/EN/VSA-Online-Help.asp?1938.htm)*. Check any of these checkboxes to perform their corresponding actions when an alarm 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

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

- **Notify user when app blocked** - Notify the user when a blocked application attempts to access the network. Use this function to build up the access list based on normal usage. This lets you see which applications on your system are accessing the network and when. The machine user is prompted to select one of four responses when an application is blocked:
  - **Always** - Allows the application access to the network indefinitely. Users will not be prompted again.
  - **Yes** - Allows the application access to the network for the duration of the session. Users will be prompted again.
  - **No** - Denies the application access to the network for the duration of the session. Users will be prompted again.
  - **Never** - Denies the application access to the network indefinitely. Users will not be prompted again.
- **Enable/Disable driver at next reboot** - **Enable/Disable** the network access protection driver for an agent. Applications that do not use the Windows TCP/IP stack in the standard way may conflict with this driver, especially older legacy applications. **The agent can not monitor network statistics or block network access if this driver is disabled.** *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

Remote Control

- **Select user notification type:**

- **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 - Working Directory

Policy Management > Policies > Settings tab > Working Directory checkbox

Working Directory

- **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 to them. Setting the deployment interval to manual requires the user to click the **Apply Now** button on the **Policies** *(page 4)* 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 19)* > **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 compliance.

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

- **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading. 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.
- **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.

- **Exclude the following time range** - **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

Clears the recurring schedule.

Organizations / Machine Groups

Policy Management > Organizations / Machine Groups

The **Organizations / Machine Groups** page assigns policies to organizations and machine groups.

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.
- **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.
- **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.
- **(Folder Tree Filters)** - Applies to **Machine Groups** cabinet and **Policies** 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 17)* 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 scroll 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.
  - The following policy types **combine with each other** so that no conflicts occur.
    - ✓ Event log alerts, distribute files, monitor sets, and agent procedures.
- Policies are assigned *by organization/machine group* using the **Organizations/Machine Groups** *(page 18)* page.
  - Policies assigned to a lower level in an organization hierarchy have precedence over policies assigned to a higher level in the same organization hierarchy.

  - Unless a lower level policy conflicts with it, policies assigned to a level apply to all lower levels.
  - 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 19)* 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 4)* 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.

Actions

- **Assign** - Assigns policies to selected machines.
- **Clear Override** - Clears KPM 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 KPM policy override condition exists if agent settings for a machine have been set manually, outside of the KPM 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. KPM policies will be ignored from then on. Clearing an override enables applied KPM 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 Machine** - Displays policies assigned by machine
- **Policies Assigned to Organizations/Machine Groups** - Displays policies assigned by organization and machine group.

Actions

- **Remove** - You can remove policies assigned to the machine.
- **Move Up and Move Down** - You can re-order the sequence of 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.
  - The following policy types **combine with each other** so that no conflicts occur.
    - ✓ Event log alerts, distribute files, monitor sets, and agent procedures.
- Policies are assigned *by organization/machine group* using the **Organizations/Machine Groups** *(page 18)* page.
  - Policies assigned to a lower level in an organization hierarchy have precedence over policies assigned to a higher level in the same organization hierarchy.
  - Unless a lower level policy conflicts with it, policies assigned to a level apply to all lower levels.
  - 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 19)* 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 4)* 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 > Service Billing - Agent Policy Status

- Displays only if the Service Billing 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 > Service Billing - Policy Info & Association

- Displays only if the Service Billing 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**

Index