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 Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer’s acceptance of the Agreement.”
Contents

Software Management Overview ................................................................. 1
Software Management Module Minimum Requirements .................................... 2
Configuring Software Management ............................................................... 2
Dashboard ..................................................................................................... 3
Machines ....................................................................................................... 3
Patch Approval ............................................................................................ 5
Vulnerabilities ............................................................................................... 5
Patch History ................................................................................................. 6
Scan and Analysis .......................................................................................... 6
  Configure Operating System Update ............................................................. 6
  Kaseya Update ............................................................................................. 7
Override ........................................................................................................ 8
3rd-Party Software ......................................................................................... 9
Deployment .................................................................................................... 10
Alerting .......................................................................................................... 11
Settings ......................................................................................................... 12
  Application Settings .................................................................................... 12
  Migration ..................................................................................................... 13
Application Logging ....................................................................................... 14
Index ............................................................................................................. 15
Software Management Overview

Software Management is a vulnerability and patch management module for Windows and Apple machines. Software Management also manages deployment of popular 3rd-party software packages for both Windows and Apple operating systems. Patches for 3rd-party software is included, if made available by 3rd-party software package developers.

Scanning and deployment can be on demand or automated across thousands of machines. Settings are assigned to machines using profiles for scanning, deployment, alerts, 3rd-party software and patch overriding. Once profiles are assigned, policy enforcement is validated using compliance checking metrics for scanning and deployment.

- **Scan and analysis profiles** support two different *strategies* for managing software updates.
  - **Configure Operating System Update** - Configures how updates for Windows and Apple machines are performed on assigned machines. Individual Windows and Apple patches are not reviewed and selected using this option. *3rd-party patches cannot be deployed using this strategy.*
  - **Kaseya Update** - Specifies whether to approve, reject or review patches based on a pre-assigned *impact classification*. This patch strategy applies to Windows, Apple and 3rd-party software patches.
- **Deployment profiles** specify how deployments occur, on a recurring schedule. This includes:
  - Reboot preferences.
  - The optional running of agent procedures both before or after deployment.
  - Optional blackout windows, to prevent scheduling deployments during business hours.
- Includes patch approvals, which lets you approve or reject specific patches.
- Supports scanning and deploying patches immediately.
- Provides a *force update* feature, which initiates a scan, then deploys all installs and approved patches immediately, rebooting as often as necessary.
- 3rd-party software profiles enable you to maintain lists of popular software titles and versions that can be installed on agent machines.
  - A Software Management license is only incremented when 3rd-party software management is enabled for an agent machine.
  - 3rd-party software can only be installed by deployment profile.
  - Requires a scan and analysis profile be assigned to the agent machine that uses the Kaseya Update strategy.
- **Patch override profiles**—by KB article, patch number, and filter criteria—can be specified. When assigned to a machine, these profiles override the default classifications assigned to patches: approved, rejected, or review.
- **Alerts** are provided for patch and configuration issues.
- A daily compliance check is run for delayed scans, delayed deployments and percentage of patches deployed.
- **Software Management activities** are tracked using reports, application logs and diagnostic logs.
- The Dashboard page includes two download links:
  - A Patches Available PDF for quarterly patch information.
  - An Installers Available PDF for installable 3rd party applications.
Software Management Module Minimum Requirements

Kaseya Server
- The **Software Management** R94 module requires VSA R94.
- An agent version must be 9.4.0.12 or later.

Configuring Software Management

1. **Scan and Analysis** *(page 6)* - Create scan and analysis profiles, on a recurring schedule. For each profile you create, you must decide on one of two *patch strategies*.
   - **Configure Operating System Update** - Configures how updates for Windows and Apple machines are performed on assigned machines. Individual Windows and Apple patches are not reviewed and selected using this option. *3rd-party patches cannot be deployed using this strategy.*
   - **Kaseya Update** - Specifies whether to approve, reject or review patches based on a pre-assigned *impact classification*. This patch strategy applies to Windows, Apple and 3rd-party software patches.
2. **Deployment** *(page 10)* - Create profiles that specify how deployments occur, on a recurring schedule. This can include running agent procedures both before or after deployment.
3. **3rd-Party Software** *(page 9)* - Assign software titles, by version number, to a 3rd-party software installation profile.
4. Optionally create patch overrides for specific patches using the **Override** *(page 8)* page.
5. Optionally create alerts using the **Alerting** *(page 11)* page.
6. Optionally enable compliance checking using the **Settings** *(page 12)* page.
7. Assign machines to the profiles you’ve created, using the **Machines** *(page 3)* page or any of the profile pages.
8. After a scan has been completed, any patch that requires review must be approved to deploy it. You can approve patches using the **Patch Approval** *(page 5)* page or **Machines** page.

Additional Guidelines

- All agents assigned a **Scan and Analysis** profile using the Kaseya Update patch strategy must have a **Deployment** profile assigned to them or patches will not be deployed.
- 3rd-party software must be enabled on the **Machines** page for 3rd-party software to be installed or patched.
- You can scan machines immediately using the **Machines** page. A machine must be assigned a **Scan and Analysis** profile.
- You can deploy patches immediately using the **Vulnerabilities** *(page 5)* page or **Machines** page.
- You can also deploy all approved patches and 3rd-party software packages assigned to a machine immediately, rebooting the machine as often as necessary, using the **Force Update** button on the **Machines** page.
Dashboard

Reports

Logs
- See Application Logging (page 14) in the Software Management module.

Dashboard

Software Management > Management > Dashboard
The Dashboard page provides a dashboard view of Software Management metrics and activities.
- Hover the cursor over any pie slice to see statistics for that pie slice.

Dashboard metrics and activities include:
- % Machines Vulnerable
- Top 5 Vulnerabilities
- Total # Vulnerabilities
- Top 10 Vulnerable Machines
- % Machines In/Out of Compliance
- # Machines Vulnerable

The Dashboard page also includes two download links:

Machines

Software Management > Management > Machines
The Machines page manages the assignment of Software Management profiles on selected machines. The Machines page can also execute a manual scan of machines, suspend and resume Software Management tasks, and remove profile assignments.

Upper Panel Actions
- Assign Profiles - Assigns profiles to selected machines.
  - Scan and Analysis (page 6)
  - Deployment (page 10)
  - 3rd-Party Software (page 9)
  - Override Profiles (page 8) - Assigns to Override profiles to selected machines.
  - Removed inherited overrides - If checked, removes all overrides already assigned.
- Remove Profiles - Removes a selected type of profile from selected machines.
- Suspend/Resume -Suspends or resumes Software Management activities on selected machines.
- Scan Now - Executes a scan on selected machines immediately. A machine must be assigned a Scan and Analysis (page 6) profile.
• **3rd-Party Support** - Enables or disables 3rd-party installations and patching for selected machines, without having to adjust the profile assigned to the machine.

• **Force Update** - Initiates a scan, then deploys all installs and approved patches immediately, rebooting as often as necessary. Ignores the Deployment (page 10) profile assigned to a machine.

• **Licensing** - Profiles Software Management license counts for 3rd-party installations and patching. Software Management license counts also display on the Administration > Manage > License Manage (http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#2924.htm) page.
  - Purchased
  - Available - Purchased not applied or expired.
  - Applied - Active license applied to a machine.
  - Expiration Date - Licensing sets the Software Management expiration date equal to the VSA maintenance expiration date.
  - # of Days Remaining - Days remaining before all licenses expire.

• **Disconnect from Patch Mgmt** - Disconnects selected agents from being managed by Patch Management.
  - A corresponding Attached to Patch Management column indicates if an agent is currently being managed by Patch Management.

• **Refresh** - Refreshes the grid.

**Upper Panel Columns**

- **Agent ID**
- **Status**
  - (†) managed by Software Management
  - (X) Software Management activities are suspended
- **Machine Id**
- **Pending Actions**
  - (green) scanning
  - (yellow) deploying a patch
  - (blue) rebooting or waiting for a reboot
  - (red) inside the blackout window
  - (triangle) warning
  - (exclamation) error
- **Vulnerabilities**
- **Scan and Analysis Profile**
- **Deployment Profile**
- **3rd-Party Software Profile**
- **3rd-Party Support** - Enabled or blank.
- **Last Scan Data**
- **Last Deploy Date**

**Lower Panel Tabs**

- **Vulnerabilities** - Profiles identified **vulnerabilities** (page 5) for the selected machine.
  - **Deploy Patches** - Schedules patch deployments for selected vulnerabilities to the selected machine.
  - **Refresh** - Refreshes the tab.
- **Profiles** - Displays the profiles assigned to the selected machine.
  - **Scan and Analysis Profile**
  - **Deployment Profile**
Patch Approval

- **3rd-Party Software Profile** - Lists the assigned software, by title and version.
- **Override Profiles** - Lists overrides. Overrides have precedence from highest to lowest in the list. You can reorder overrides for the selected machine using the **Move Up** or **Move Down** buttons. You can also **Delete** an override for the selected machine.

- **Pending Patches** - Profiles the pending patches set to **Review** by the latest **Scan and Analysis** (page 6) scan of a machine. See **Patch Approval** (page 5).
  - **Approve** - Approves pending patches for deployment.
  - **Reject** - Rejects pending patches for deployment. Rejected patches can be subsequently approved and deployed using the **History** tab.

- **Errors** - Profiles **Software Management** task errors for a selected machine.
  - **Delete** - Deletes a reported error. Deleted errors can still be identified in Agent > **Agent Logs** (http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#354.htm) > Diagnostic Logs > Endpoints > **Software Management Logs**
  - **History** - Shows the history of completed and rejected patches.
  - **Approve** - Approves selected rejected patches.

---

**Patch Approval**

**Software Management > Management > Patch Approval**

The **Patch Approval** page approves pending patches set to **Review** by the latest **Scan and Analysis** (page 6) scan of a machine or any assigned **Overrides Profiles** (page 8).

- **Approve** - Approves pending patches for deployment.
- **Reject** - Rejects pending patches for deployment. Rejected patches can be subsequently approved and deployed using the History tab on the **Machines** (page 3) page.

**Actions**

- **Approve**
- **Reject**

---

**Vulnerabilities**

**Software Management > Management > Vulnerabilities**

The **Vulnerabilities** page lists the vulnerabilities discovered on all **scanned** (page 6) machines in the VSA. If you have chosen a 3rd-party vulnerability and your machine does not allow for 3rd-party patching on the **Machines** (page 3) page then it will not be deployed.

Vulnerabilities are security risks associated with a machine. They can include the configuration of the operating system, applications, firewall settings, browser plugins and extensions, antivirus and antimalware support, removable devices, scripts and macros, etc. A vulnerability is no longer displayed for a machine once scanning confirms the corresponding install or patch has been deployed to the machine.

**Actions**

- **Deploy Patches** - Schedules patch deployments for selected vulnerabilities to selected machines.
Patch History

Software Management > Management > Patch History

The Patch History page shows the history all approved and rejected patches for a selected profile. Select the hyperlink of a listed patch to view its details.

- Approved Patches
- Rejected Patches
  - Approve - Approves selected rejected patches.
- Gear Icon
  - Export - Exports the selected profile's patch history.
  - Refresh - Refreshes the list.
  - Reset - Clears any filtering set for this list.

Scan and Analysis

Software Management > Profiles > Scan and Analysis

The Scan and Analysis page creates profiles that specify the patch strategy used to select patches for deployment. A Scan and Analysis profile also specifies when a scan runs on a recurring schedule. A scan can always be run immediately using the Scan Now button on the Machines (page 3) page.

Patch Strategies

A Scan and Analysis profile specifies one of two patch strategies to select and deploy patches.

- Configure Operating System Update (page 6)
- Kaseya Update (page 7)

Actions

- New - Creates a Scan and Analysis profile, using one of two patch strategies described above.
- Edit - Edits a selected profile.
- Delete - Deletes the selected profile.
- Refresh - Refreshes the grid.

Machines Assigned

Machines can also be assigned profiles using the Machines (page 3) page.

- Assign - Assigns selected machines to a profile. A machine can only be assigned one profile at a time.
- Remove - Removes selected machines from a profile.

Configure Operating System Update

Software Management > Profiles > Scan and Analysis

The Configure Operating System Update Patch Strategy configures how updates for Windows and Apple machines are performed on assigned machines.

- Individual Windows and Apple patches are not reviewed and selected using this option.
- Third-party patches cannot be deployed using this strategy.
Using this strategy takes effect as soon as the machine is assigned to the profile, and wherever the profile is updated.

When this patch strategy is selected, the following additional options display:

- **Operating System Update**
  - Ask user to download and install
  - Automatically download and ask user to install
  - Automatically download and schedule installation
  - Require automatic updates but let user configure
  - Turn off Operating System Update

- **Schedule on** - Specifies when the OS should check for updates.
- **Reboot** - If any of the OS patches installed require a reboot:
  - Force reboot if user is logged in
  - Do not force reboot

**Mac OS Update Settings**

The following Mac OS settings are checked in the System Preferences > Apple Store dialog for each Operating System Update value selected in Software Management.

<table>
<thead>
<tr>
<th>In Software Management</th>
<th>Ask user to download and install</th>
<th>Automatically download and ask user to install</th>
<th>Automatically download and schedule installation</th>
<th>Require automatic updates but let user configure</th>
<th>Turn off Operating System Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically check for updates</td>
<td>〇</td>
<td>〇</td>
<td>〇</td>
<td>〇</td>
<td></td>
</tr>
<tr>
<td>Download Newly available updates in Background</td>
<td>〇</td>
<td>〇</td>
<td>〇</td>
<td>〇</td>
<td></td>
</tr>
<tr>
<td>Install app updates</td>
<td>〇</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install OS X updates</td>
<td>〇</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install system data files and security updates</td>
<td>〇</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Kaseya Update**

Software Management > Profiles > Scan and Analysis

A profile using the Kaseya Update Patch Strategy specifies whether to approve, reject or review patches using a pre-assigned impact classification. Reviewed and rejected patches can be subsequently approved, using either the Patch Approval (page 5) page or the Machines (page 3) page.

- All agents assigned a Scan and Analysis profile using the Kaseya Update patch strategy must have a Deployment (page 10) profile assigned to them or patches will not be deployed.
Override

- This patch strategy applies to Microsoft, Apple and 3rd-party software title patches.

When this patch strategy is selected, the following additional options display:

- **Patch Impact** - Sets the criteria to Approve, Review or Reject patches, by patch impact classification.
  - Critical
  - Critical, Older than 30 Days
  - Critical, Superseded
  - Recommended
  - Virus Removal

- **Schedule**
  - **Time Frame** - Daily, Weekly, Monthly
    - If Daily is selected, **Run Every X Days** displays. Enter the interval of days run.
    - If Weekly is selected, **Sunday through Saturday** displays. Select the days of the week to run.
    - If Monthly is selected, **Run Every X Months** displays. Enter additional parameters to specify the interval of months to run and when to run during a month.
  - **Scan Run Time (agent time)** - Enter the agent time to run.

Override

**Software Management > Profiles > Override**

The **Override** page specifies *named sets* of selected overrides. An override exists for each patch that can be deployed. These overrides, if assigned to a machine, take precedence over the approval, review or rejection of these same patches assigned to a machine by **Scan and Analysis (page 6)** or **3rd-Party Software (page 9)** profile. Overrides are assigned to machines using the **Assign Profiles** button on the **Machines (page 3)** page.

Overrides have precedence from highest to lowest in each override list. On the **Override** page you can reorder overrides by dragging and dropping them within a list during editing. Once an override list is assigned to a machine on the **Machines (page 3)** page, you can adjust the order of overrides for each machine separately or **Delete** an override for an individual machine.

You can specify overrides using three tabs.

**KB Override tab**

Specifies overrides for patches identified by Microsoft KB number.

- **New** - Opens a dialog to specify a KB patch override profile.
  - **Name** - The name of the override profile.
  - **Add Row** - Adds a new row. For a row select Approve or Reject or Review. Then select the KB patch.
  - **Delete Row** - Deletes a selected row.
- **Edit** - Edits an existing override profile.
- **Delete** - Deletes an override profile.

**Patch Override tab**

Specifies overrides for patches not identified by Microsoft KB number.

- **New** - Opens a dialog to specify a patch override profile.
  - **Name** - The name of the override profile.
3rd-Party Software

- **Add Row** - Adds a new row. For a row select Approve or Reject or Review. Then select the patch.
- **Delete Row** - Deletes a selected row.
- **Edit** - Edits an existing override profile.
- **Delete** - Deletes an override profile.

**Advanced Overrides tab**

Specifies overrides using custom filtering.

- **New** - Opens a dialog to specify a patch override profile by custom filtering.
  - **Name** - The name of the override profile.
  - **Add Row** - Adds a new row. For a row enter values for:
    - **Approve/Reject** - Select Approve or Reject or Review.
    - **Field** - CVE Code, Name, Description, Vendor, Product. A CVE Code refers to a Common Vulnerabilities and Exposures identifier for a patch.
    - **Operator** - Equals, Not equal to, Contains, Does not contain. Like matches if the value entered is contained in the field.
    - **Value** - Enter any string to filter by.
  - **Delete Row** - Deletes a selected row.
- **Edit** - Edits an existing override profile.
- **Delete** - Deletes an override profile.

---

3rd-Party Software

Software Management > Profiles > 3rd-Party Software

The 3rd-Party Software page assigns software titles, by version number, to a profile. 3rd-Party Software profiles are then assigned to machines using either this page or the Assign Profiles button on the Machines (page 3) page. Software titles are deployed based on the schedule specified by a machine’s assigned Deployment (page 10) profile. 3rd party software cannot be deployed on demand.

**Actions**

- **New** - Opens a profile dialog that specifies a list of software titles, by vendor, title and version.
  - **Name**
  - **Description**
  - **Add** - Opens a dialog to search for and add software titles and versions. You cannot add two versions of the same software title to the profile.
  - **Delete** - Deletes a software title and version from the profile.
- **Edit** - Edits an existing profile.
- **Delete** - Deletes a profile.
- **Refresh** - Refreshes the grid.

**Machines Assigned**

- **Assign** - Assigns selected machines to a profile. A machine can only be assigned one profile at a time.
- **Remove** - Removes selected machines from a profile.
Deployment

Software Management > Profiles > Deployment

The Deployment page creates profiles that specify how and when deployments are executed on assigned machines. The deployment profile can be assigned on this page or on the Machines (page 3) page.

Actions
- **New** - Creates a Deployment profile.
- **Edit** - Edits a selected profile.
- **Delete** - Deletes the selected profile.
- **Refresh** - Refreshes the grid.

Machines Assigned
Machines can also be assigned profiles using the Machines (page 3) page.
- **Assign** - Assigns selected machines to a profile. A machine can only be assigned one profile at a time.
- **Remove** - Removes selected machines from a profile.

Deployment Profile Options

Reboot Options
Reboot prompts and warnings occur after the install.
- **When the user is logged in**
  - Reboot immediately after update
  - Warn user and wait for x min and then reboot
  - Ask user about reboot and offer to delay (reask every x minute); do not reboot until get response
  - Ask permission, if no response in x min reboot
  - Skip Reboot
  - Do not reboot after update, send email - You can configure the email format using the Settings (page 12) page.
- **Wait time** - Minutes to wait after warning the user of reboot.
- **When a user is not logged in**
  - Reboot immediately after update
  - Warn user and wait for x min and then reboot
  - Skip Reboot
  - Do not reboot after update, send email - You can configure the email format using the Settings (page 12) page.

Procedures
The following options select an agent procedure to run before or after an update or reboot.
- **Pre-Update Procedure**
- **Pre-Reboot Procedure**
- **Post-Update Procedure**
- **Post-Reboot Procedure**

Schedule
Schedules recurring deployments. The recurring schedule for a deployment typically follows the recurring schedule for a Scan and Analysis (page 6) scan by at least several hours.
Alerting

- **Time Frame** - Daily, Weekly, Monthly
  - If Daily is selected, **Run Every X Days** displays. Enter the interval of days run.
  - If Weekly is selected, **Sunday through Saturday** displays. Select the days of the week to run.
  - If Monthly is selected, **Run Every X Months** displays. Enter additional parameters to specify the interval of months to run and when to run during a month.

- **Run Time** - Enter the agent time to run.

**Blackout Window**
Blackout windows prevent schedule deployments from being run during specified days/times of the week. A scheduled run time can only be specified outside of a blackout window.

- **Monday - Friday**
  - **Start Time**
  - **End Time** - Includes a Do not restart until the next profile time value. This value extends the blackout window until the next time the deployment profile is scheduled to run.

- **Saturday - Sunday**
  - **Start Time**
  - **End Time**

---

### Alerting

**Software Management > Profiles > Alerting**

The **Alerts** page manages **Software Management** patch alert profiles. Each alert profile represents a different set of alert conditions and actions taken in response to an alert. Multiple alert profiles can be assigned to an endpoint concurrently. Changes to an alert profile affect all machine IDs assigned that alert profile. Different types of machines may require different alert profiles. Alert profiles are visible to all VSA users. Alerts are processed every six hours.

**Reviewing Alarms Created by Software Management Alerts**

- The Agent > Agent Logs > **Monitor Action Log** ([http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#354.htm](http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#354.htm)) - Shows the actions taken in response to an alert, whether or not an alarm was created.

**Actions**

- **New** - Creates a new alert profile.
- **Edit** - Edits an existing alert profile. You can also double-click an alert profile to open it.
- **Delete** - Deletes an existing alert profile.
- **Copy** - Saves a selected alert profile with new name.
- **Alerts Configuration** - Configures the format of an alert notification message.

**Summary tab**
The **Summary** tab sets basic options about an alert profile and how duplicate alerts are filtered.

- **Name** - The name of the alert profile.
- **Description** - A description of the alert profile.
Settings

- **Filter duplicate alerts** - Prevents duplicate alerts from being generated for a specified number of time periods.
  - **Time Frame** - Days, Hours, Minutes
  - **Every X days/hours/minutes** - Number of days, hours, or minutes to suppress duplicate alerts.

Alert Types tab

The **Alerts Types** tab specifies the conditions that cause an **Software Management** alert to be created. The format for notifying users about each alert type can be changed using the **Alerts Configuration** button.

- **New patch is available**
- **Patch install fails**
- **Windows Auto Update changed** - The machine user changes Windows Auto Update settings.

Actions tab

The **Actions** tab of an alert profile determines the actions taken in response to any of the **Alert Types** encountered by an endpoint assigned that alert profile.

- **Create Alarm** - If checked and an alert type is encountered, an alarm is created.
- **Create Ticket** - If checked and an alert condition is encountered, a ticket is created.
- **Email Recipients (comma separated)** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- **Script Name to Run** - If an alert condition is encountered, run the selected agent procedure.
- **Users Notified in Info Center** - If checked and an alert condition is encountered, a notification is sent to the specified user's Info Center > Inbox
- **Send Message to Notification Bar** - If checked and an alert condition is encountered, a notification is sent to the specified user's Notification Bar

Endpoints tab

The **Endpoints** tab lists all machines using the selected alerts profile.

- **Add** - Assigns the alert profile to selected machines.
- **Delete** - Removes an alert profile assignment from selected machines.

Settings

**Software Management > Configuration > Settings**

The **Settings** page sets options for the entire module in two tabs.

Application Settings

**Software Management > Configuration > Settings > Application Settings**

The **Application Settings** tab sets general options for the entire module.

Actions

- **Edit**
  - **Reboot Action Email** - Applies only if Do not reboot after update, send email is selected in a Deployment (page 10) profile. Specifies the **Subject** and **Body** format of email notifications that a machine needs to be rebooted after a patch.
Settings

- **Compliance** - Compliance checking is reported on the [Dashboard](http://help.kaseya.com/webhelp/EN/vsa/9040000/index.asp#10631.htm) (page 3) page and in Info Center > Report Parts for **Software Management**.
  - **Compliance Check** - Specifies how often machines are checked for compliance, based on Kaseya Server time.
  - **Scan Grace Period** - Specifies the grace period included in compliance checking for scanning. A machine is out of compliance if—at the time compliance is checked—the last actual scan was later than the last scheduled scan plus the grace period.
  - **Deploy Grace Period** - Specifies the grace period included in compliance checking for deployment. A machine is out of compliance if—at the time compliance is checked—the last actual deployment was later than the last scheduled deployment plus the grace period.
  - **Patch Tolerance** - Specifies a percentage ratio of deployed patches to approved patches. A machine is out of compliance if deployed patches are less than the specified percentage of approved patches.

**Note:** 3rd-party patches are only included in compliance calculations if 3rd-party patching has been enabled for a machine.

- **Prevent an agent from running both Patch Management and Software Management at the same time** - If checked, **Software Management** will not run **Scan Now** on an agent if that agent is configured to use any of these **Patch Management** features:
  - Patch Management Policy
  - Scan Schedule
  - Automatic Update Schedule
  - Machine Update Schedule
  - Patch Update Schedule

Migration

Software Management > Configuration > Settings > Migration

The **Migration** tab enables you to migrate policies from **Patch Management** to **Software Management**. There are two types of migration.

- **Migrate Knowledge Base Overrides**
- **Migrate Policies**

**Migrating Knowledge Base Overrides**

This option migrates all global KB overrides specified using the [Patch Management > KB Override](http://help.kaseya.com/webhelp/EN/KPATCH/9040000/index.asp#3901.htm) page. The migration creates a new KB override profile (page 8) in **Software Management** with the name you specify.

**Note:** You can only perform this migration once.

1. Click the **Migrate Knowledge Base Overrides** button.
2. Enter a **Knowledge Base Override Name**.
3. Click **Convert**.

**Migrating Policies**

This option migrates [Patch Management policies](http://help.kaseya.com/webhelp/EN/KPATCH/9040000/index.asp#2173.htm). Optionally migrates machine associations. This migration creates a new KB override profile (page 8) in **Software Management** with
the name you specify. Click the Migrate Policies button. 
1. In the dialog select one or more policies.
   - Policy
   - Copy Approvals
   - Copy Denials
   - Copy Machine Associations
2. Click Convert.

Application Logging

Software Management > Administration > Application Logging

The Application Logging page displays a log of Software 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.
Index

3
3rd-Party Software • 9

A
Alerting • 11
Application Logging • 14
Application Settings • 12

C
Configure Operating System Update • 6
Configuring Software Management • 2

D
Dashboard • 3
Deployment • 10

K
Kaseya Update • 7

M
Machines • 3
Migration • 13

O
Override • 8

P
Patch Approval • 5
Patch History • 6

S
Scan and Analysis • 6
Settings • 12
Software Management Module Minimum Requirements • 2
Software Management Overview • 1

V
Vulnerabilities • 5