Software Management

User Guide

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in CloudActiv8's "Click-Accept" EULA as updated from time to time by CloudActiv8 at http://www.CloudActiv8.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from CloudActiv8 as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

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 overrides. 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.*
  - **CloudActiv8 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 CloudActiv8 Update strategy.
- Patch override profiles—by 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

- An agent version must be 9.4.0.12 or later.
- Applies to **Windows and Apple supported agents**. Patches for Windows 7are provided up until January 2020 (Extended Support patches are not supported).
- Depending on the various operating systems managed, up to 200 GB of storage should be free to store patches.

Configuring SoftwareManagement

1. **Scan and Analysis** *(page vi)* - 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.*
   - **CloudActiv8 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** - 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** - 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.
5. Optionally create alerts using the **Alerting** page.
6. Optionally enable compliance checking using the **Settings** page.
7. Assign machines to the profiles you've created, using the **Machines** 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 or **Machines** page.

Additional Guidelines

- All agents assigned a **Scan and Analysis** profile using the CloudActiv8 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 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.

Reports

- A category of report parts for Software Management is provided on the Info Center > Configure & Design > **Report Parts** page.

Logs

- See **Application Logging** in the Software Management module.
- A Software Management diagnostic log is provided on the Agent > Agents > **Agent Logs** > Diagnostic Logs > Endpoint tab.

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**

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**
  - **Deployment**
  - **3rd-Party Software**
  - **Override Profiles** - 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** 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** 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** 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 CloudActiv8 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**
  - **Software Management** activities are suspended
- **Machine Id**
- **Pending Actions**
  - scanning deploying a patch
  - rebooting or waiting for a reboot
  - inside the blackout window
  - warning 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** 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**
  - **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** scan of a machine. See **Patch Approval** .
  - **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** > Diagnostic Logs > Endpoints> **Software Management Logs**
- **History** - Shows the history of completed and rejected patches.
  - **Approve** - Approves selected rejected patches.
    - ✓ **Status** - Can be Completed or Rejected. Completed means it was patched successfully. Rejected means either the patch is rejected in the Scan and Analysis profile, or it was rejected manually from Pending Patches tab.
    - ✓ **Status Date** - The date the patch was put in Completed or Rejected status.

Patch Approval

Software Management > Management > Patch Approval

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

- **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.

Actions

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

Vulnerabilities

Software Management > Management > Vulnerabilities

The **Vulnerabilities** page lists the vulnerabilities discovered on all **scanned** machines in the CloudActiv8. If you have chosen a 3rd-party vulnerability and your machine does not allow for 3rd-party patching on the **Machines** 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 > New/Edit

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.

Patch Strategies

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

- **Only OS Updates**
- **Third-Party Software Updates + OS Updates**
- **CloudActiv8 Update**

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.

- **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.

Only OS Updates

Software Management > Profiles > Scan and Analysis

The 'Only OS Updates' 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. Use "Third Party Software Updates + OS Updates" strategy if you want to configure 3rd-party software updates as well.
- Using this strategy takes effect as soon as the machine is assigned to the profile. Wherever the profile is updated.

When this patch strategy is selected, two sections appear:

- Configure Windows Group Policies Related to Windows Update
- Mac OS Update Settings

Configure Windows Group Policies Related to Windows Update

This section contains all Windows Group Policies related to Windows Updates. They can be configured in CloudActiv8 in a similar way to what an administrator will do on a Domain Controller if their organization uses Active Directory.

Policy can have following statuses:

- **Enabled** - Windows behaves in the way specified by the policy and it uses the specified options if there are any. Endpoint user is not able to modify those settings in "Windows Update" application.
- **Disabled** - The policy is turned off and endpoint user is not able to modify those settings in "Windows Update" application.
- **Not Configured** - The policy is turned off, but endpoint user is able to modify those settings in "Windows Update" application.
- Some policies contain variables and/or values required such as but not limited to: (hours, minutes, days)

After unassigning a machine from the profile all policies are set back to **Not Configured** status (default Windows configuration).

Windows policies configured in this section are applied on a machine level. It means that if an endpoint user configured any of the policies listed in this section, their configuration will be overridden when the scan and analysis profile is applied. However, this configuration has lower priority than Windows Policies configured by an administrator on a domain controller (in case their organization uses Active Directory).

To understand the Native Windows Patching Controls Configuration from Microsoft, please click **here** *(https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-architecture)*.

Configure Automatic Updates Policy

This policy specifies whether the computer will receive security updates and other important downloads through the Windows automatic updating service.

Policy can have following statuses:

- **Enabled** – This option specifies that local administrators will be allowed to use the Windows Update control panel to select a configuration option of their choice. However, local administrators will not be allowed to disable the configuration for Automatic Updates.
- **Disabled** - If this option is selected, any updates that are available on Windows Update must be downloaded and installed manually. To do this, search for Windows Update using Start.
- **Not Configured** – If this option is selected, use of Automatic Updates is not specified at the Group Policy level. However, an administrator can still configure Automatic Updates through Control Panel.

Turn on recommended updates via Automatic Updates

This policy specifies whether Automatic Updates will deliver both important as well as recommended updates from the Windows Update service.

Policy can have following statuses:

- **Enabled** – If this option is selected, Automatic Updates will install recommended updates as well as important updates from Windows Update service.
- **Disabled** - If this option is selected, Automatic Updates will continue to deliver important updates if it is already configured to do so.
- **Not Configured** - If this option is selected, Automatic Updates will continue to deliver important updates if it is already configured to do so.

Automatic Updates detection frequency

This policy specifies the hours that Windows will use to determine how long to wait before checking for available updates.

Policy can have following statuses:

- **Enabled** – If this option is selected, Windows will check for available updates at the specified interval.
  - **Interval (hours)** - The exact wait time is a sum of the specific value and a random variant of 0-4 hours.
- **Disabled** - If this option is selected, Windows will check for available updates at the default interval of 22 hours.
- **Not Configured** - If this option is selected, Windows will check for available updates at the default interval of 22 hours.

Allow Automatic Updates immediate installation

This policy specifies whether Automatic Updates should automatically install certain updates that neither interrupt Windows services nor restart Windows.

Policy can have following statuses:

- **Enabled** – If this option is selected, Automatic Updates will immediately install these updates once they are downloaded and ready to install.
- **Disabled** - If this option is selected, Automatic Updates will not be installed immediately.
- **Not Configured** - If this option is selected, Automatic Updates will not be installed immediately.

Allow signed updates from an intranet Microsoft update service location

This policy specifies whether Automatic Updates accepts updates signed by entities other than Microsoft when the update is found on an intranet Microsoft update service location.

Policy can have following statuses:

- **Enabled** – If this option is selected, Automatic Updates accepts updates received through an intranet Microsoft update service location, if they are signed by a certificate found in the "Trusted Publishers" certificate store of the local computer.
- **Disabled** – If this option is selected, Automatic Updates from an intranet Microsoft update service location must be signed by Microsoft.
- **Not Configured** – If this option is selected, Automatic Updates from an intranet Microsoft update service location must be signed by Microsoft.

Delay restart for scheduled installations

This policy specifies the amount of time Automatic Updates will wait before proceeding with a scheduled restart.

Policy can have following statuses:

- **Enabled** – If this option is selected, a scheduled restart will occur after the specified number of minutes has expired.
  - **Restart (minutes)** - Specifies the amount of time (in minutes) Automatic Updates waits before proceeding with a scheduled restart.
- **Disabled** - If this option is selected, the default wait time of fifteen minutes will elapse before any scheduled restart occurs.
- **Not Configured** - If this option is selected, the default wait time of fifteen minutes will elapse before any scheduled restart occurs.

Enabling Windows Update Power Management to automatically wake up the computer to install scheduled updates

This policy specifies whether the Windows Update will use the Windows Power Management features to automatically wake up the system from hibernation, if there are updates scheduled for installation.

Policy can have following statuses:

- **Enabled** – If this option is selected, Windows Update will only automatically wake up the system if Windows Update is configured to install updates automatically. If the system is in hibernation when the scheduled install time occurs and there are updates to be applied, then Windows Update will use the Windows Power management features to automatically wake the system up to install the updates.
- **Disabled** - If this option is selected, the system will not wake unless there are updates to be installed. If the system is on battery power, when Windows Update wakes it up, it will not install updates and the system will automatically return to hibernation in 2 minutes.
- **Not Configured** - If this option is selected, Windows Update does not wake the computer from hibernation to install updates.

No auto-restart with logged on users for scheduled automatic updates installations

This policy specifies that to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted by any user who is logged on, instead of causing the computer to restart automatically.

Policy can have following statuses:

- **Enabled** – If this option is selected, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged in to the computer. Instead, Automatic Updates will notify the user to restart the computer.
- **Disabled** - If this option is selected, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation.
- **Not Configured** - If this option is selected, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation.

Re-prompt for restart with scheduled installations

This policy specifies the amount of time for Automatic Updates to wait before prompting again with a scheduled restart.

Policy can have following statuses:

- **Enabled** – If this option is selected, a scheduled restart will occur the specified number of minutes after the previous prompt for restart was postponed.
  - **Restart (minutes)** - specifies the number of minutes after the previous prompt.
- **Disabled** - If this option is selected, the default interval is 10 minutes.
- **Not Configured** - If this option is selected, the default interval is 10 minutes.

Do not display `Install Updates and Shut Down` option in Shut Down Windows dialog box

This policy allows to manage whether the 'Install Updates and Shut Down' option is displayed in the Shut Down Windows dialog box.

Policy can have following statuses:

- **Enabled** – If this option is selected, the 'Install Updates and Shut Down' will not appear as a choice in the Shut Down Windows dialog box, even if updates are available for installation when the user selects the Shut Down option in the Start menu.
- **Disabled** - If this option is selected, the 'Install Updates and Shut Down' option will be available in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.
- **Not Configured** - If this option is selected, the 'Install Updates and Shut Down' option will be available in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

Do not adjust default option to `Install Updates and Shut Down` in Shut Down Windows dialog box

This policy allows to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog.

Policy can have following statuses:

- **Enabled** – If this option is selected, the user's last shut down choice (Hibernate, Restart, etc.) is the default option in the Shut Down Windows dialog box, regardless of whether the 'Install Updates and Shut Down' option is available in the 'What do you want the computer to do?' list.
- **Disabled** - If this option is selected, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.
- **Not Configured** - If this option is selected, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

Turn on Software Notifications

This policy allows to control whether users see detailed enhanced notification messages about featured software from the Microsoft Update service. Enhanced notification messages convey the value and promote the installation and use of optional software. This policy setting is intended for use in loosely managed environments in which you allow the end user access to the Microsoft Update service. By default, this policy setting is disabled.

Policy can have following statuses:

- **Enabled** – If this option is selected, a notification message will appear on the user's computer when featured software is available. The user can click the notification to open the Windows Update Application and get more information about the software or install it. The user can also click "Close this message" or "Show me later" to defer the notification as appropriate.
- **Disabled** - If this option is selected, Windows 7 users will not be offered detailed notification messages for optional applications, and Windows Vista users will not be offered detailed notification messages for optional applications or updates.
- **Not Configured** - If this option is selected, Windows 7 users will not be offered detailed notification messages for optional applications, and Windows Vista users will not be offered detailed notification messages for optional applications or updates.

Always automatically restart at the scheduled time

This policy specifies a restart timer always begins immediately after Windows Update installs important updates, instead of first notifying users on the login screen for at least two days.

Policy can have following statuses:

- **Enabled** – If this option is selected, a restart timer will always begin immediately after Windows Update installs important updates, instead of first notifying users on the login screen for at least two days.
  - **Work (minutes)** - configures the restart timer to start with any value from 15 to 180 minutes. When the timer runs out, the restart will proceed even if the PC has signed-in users.
- **Disabled** - If this option is selected, Windows Update will not alter its restart behavior.
- **Not Configured** - If this option is selected, Windows Update will not alter its restart behavior.

Do not connect to any Windows Update Internet locations

This policy specifies to not retrieve information from the public Windows Update service to enable future connections to Windows Update, and other services like Microsoft Update or the Windows Store, when Windows Update is configured to receive updates from an intranet update service.

Policy can have following statuses:

- **Enabled** – If this option is selected, it will disable functionality to retrieve information from the public Windows Update service, and may cause connection to public services such as the Windows Store to stop working.
- **Disabled** - If this option is selected, it will not disable functionality to retrieve information from the public Windows Update service.
- **Not Configured** - If this option is selected, it will not disable functionality to retrieve information from the public Windows Update service.

Select when Preview Builds and Feature Updates are received

This policy specifies the level of Preview Build or Feature Updates to receive.

Policy can have following statuses:

- **Enabled** – If this option is selected, it specifies the level of Preview Build or Feature Updates to receive, and when.
  - Select the Windows readiness level for the updates you want to receive -
    - ✓ **Preview Build - Fast**: Devices set to this level will be the first to receive new builds of Windows with features not yet available to the general public. Select Fast to participate in identifying and reporting issues to Microsoft and provide suggestions on new functionality.

      Preview Build - Slow: Devices set to this level receive new builds of Windows before they are available to the general public, but at a slower cadence than those set to Fast, and with changes and fixes identified in earlier builds.
    - ✓ **Release Preview**: Receive builds of Windows just before Microsoft releases them to the general public.
    - ✓ **Semi-Annual Channel (Targeted)**: Receive feature updates when they are released to the general public.
    - ✓ **Semi-Annual Channel**: Feature updates will arrive when they are declared Semi-Annual Channel. This usually occurs about 4 months after Semi-Annual Channel (Targeted), indicating that Microsoft, Independent Software Vendors (ISVs), partners and customer believe that the release is ready for broad deployment.
  - **After a Preview Build or Feature Update is released, defer receiving it for this many days** - You can defer receiving Preview Builds for up to 14 days.
  - **Pause Preview Builds or Feature Updates starting (format yyyy-mm-dd example 2019-10-30)** - To prevent Preview Builds from being received on their scheduled time, you can temporarily pause them. The pause will remain in effect for 35 days from the start time provided. To resume receiving Feature Updates which are paused, clear the start date field.
- **Disabled** - If this option is selected, Windows Update will not alter policy behavior.
- **Not Configured** - If this option is selected, Windows Update will not alter policy behavior.

Select when Quality Updates are received

This policy specifies when to received Quality Updates.

Policy can have following statuses:

- **Enabled** – If this option is selected, specifies when to receive quality updates.
  - **After a quality update is released, defer receiving it for this many days** – You can defer receiving quality updates for up to 30 days.
  - **Pause Quality Updates starting** – To prevent quality updates from being received on their scheduled time, you can temporarily pause quality updates. The pause will remain in effect for 35 days or until you clear the start date field.
- **Disabled** - If this option is selected, Windows Update will not alter policy behavior.
- **Not Configured** - If this option is selected, Windows Update will not alter policy behavior.

Allow updates to be downloaded automatically over metered connections

This policy specifies whether or not to download updates automatically, even over metered data connections.

Policy can have following statuses:

- **Enabled** – If this option is selected, the updates will be automatically downloaded, even over metered data connections.
- **Disabled** - If this option is selected, the updates will not be automatically downloaded.
- **Not Configured** - If this option is selected, the updates will not be automatically downloaded.

Turn off auto-restart for updates during active hours

This policy specifies the PC not to restart automatically after updates during active hours. If any of the following two policies are enabled, this policy has no effect:

1. No auto-restart with logged on users for scheduled automatic updates installations.

Always automatically restart at scheduled time.

Policy can have following statuses:

- **Enabled** – If this option is selected, the PC will not automatically restart after updates during active hours. The PC will attempt to restart outside of active hours.
  - **Start** – specifies the start time for updates.
  - **End**- specifies the end time for updates.
- **Disabled** - If this option is selected, the user selected active hours will be in effect.
- **Not Configured** - If this option is selected, the user selected active hours will be in effect.

Specify intranet Microsoft update service location

This policy specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

Policy can have following statuses:

- **Enabled** – If this option is selected, the Automatic Updates client connects to the specified intranet Microsoft update service (or alternate download server), instead of Windows Update, to search for and download updates.
  - **Set the intranet update service for detecting updates** - specifies a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.
  - **Set the intranet statistics server** - specifies a server on your network to function as an intranet statistics server.

- **Set the alternate download server** – specifies the Windows Update Agent to download files from an alternative download server instead of the intranet update service.
- **Download files with no URL in the metadata if alternate download server is set** - allows content to be downloaded from the Alternate Download Server when there are no download URLs for files in the update metadata. This option should only be used when the intranet update service does not provide download URLs in the update metadata for files which are present on the alternate download server. This option is only used if the "Alternate Download Server" is set.

- **Disabled** - If this option is selected, and if Automatic Updates is not disabled by policy or user preference, the Automatic Updates client connects directly to the Windows Update site on the Internet.
- **Not Configured** - If this option is selected, and if Automatic Updates is not disabled by policy or user preference, the Automatic Updates client connects directly to the Windows Update site on the Internet.

Configure auto-restart reminder notifications for updates

This policy specifies when auto-restart reminders are displayed.

Policy can have following statuses:

- **Enabled** – If this option is selected, you must specify the period to notify the user.
  - **Period (min)** - specifies the amount of time prior to a scheduled restart to notify the user.
- **Disabled** - If this option is selected, the default period will be used.
- **Not Configured** - If this option is selected, the default period will be used.

Configure auto-restart required notification for updates

This policy specifies the method by which the auto-restart required notification is dismissed.

Policy can have following statuses:

- **Enabled** – If this option is selected, you must specify method by which the auto-restart required notification is dismissed. When a restart is required to install updates, the auto-restart required notification is displayed. By default, the notification is automatically dismissed after 25 seconds.
  - **Method** – must be set to require user action to dismiss the notification.
- **Disabled** - If this option is selected, the default method will be used.
- **Not Configured** - If this option is selected, the default method will be used.

Configure auto-restart warning notifications schedule for updates

This policy allows to control when notifications are displayed to warn users about a scheduled restart for the update installation deadline.

Policy can have following statuses:

- **Enabled** – If this option is selected, notifications are displayed to warn users about a scheduled restart for the update installation deadline. Users are not able to postpone the scheduled restart once the deadline has been reached and the restart is automatically executed.

- **Reminder (hours)** - specifies the amount of time prior to a scheduled restart to display the warning reminder to the user.
- **Warning (mins)** - the amount of time prior to a scheduled restart to notify the user that the auto restart is imminent to allow them time to save their work.

- **Disabled** - If this option is selected, the default notification behaviors will be used.
- **Not Configured** - If this option is selected, the default notification behaviors will be used.

Maximum Background Download Bandwidth (percentage)

This policy specifies the maximum background download bandwidth that Delivery Optimization uses across all concurrent download activities as a percentage of available download bandwidth.

Policy can have following statuses:

- **Enabled** – If this option is selected, the maximum background download bandwidth that Delivery Optimization uses across all concurrent download activities as a percentage of available download bandwidth.
  - **Maximum Background Download Bandwidth (percentage)** - The default value 0 (zero) means that Delivery Optimization dynamically adjusts to use the available bandwidth for background downloads.
- **Disabled** - If this option is selected, the maximum background download bandwidth that Delivery Optimization does not use across all concurrent download activities as a percentage of available download bandwidth.
- **Not Configured** - If this option is selected, the maximum background download bandwidth that Delivery Optimization does not use across all concurrent download activities as a percentage of available download bandwidth.

Maximum Foreground Download Bandwidth (percentage)

This policy specifies the maximum foreground download bandwidth that Delivery Optimization uses across all concurrent download activities as a percentage of available download bandwidth.

Policy can have following statuses:

- **Enabled** – If this option is selected, the maximum background download bandwidth that Delivery Optimization uses across all concurrent download activities as a percentage of available download bandwidth.
  - **Maximum Foreground Download Bandwidth (percentage)** - The default value 0 (zero) means that Delivery Optimization dynamically adjusts to use the available bandwidth for foreground downloads.
- **Disabled** - If this option is selected, the maximum background download bandwidth that Delivery Optimization does not use across all concurrent download activities as a percentage of available download bandwidth.
- **Not Configured** - If this option is selected, the maximum background download bandwidth that Delivery Optimization does not use across all concurrent download activities as a percentage of available download bandwidth.

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**.

	In Software Management				
	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
Automatically check for updates	●	●	●	●	
Download Newly available updates in Background		●	●	●	
Install app updates			●		
Install OS X updates			●		
Install system data files and security updates			●		

Third-PartySoftwareUpdates+OSUpdates

Software Management > Profiles > Scan and Analysis

The Third-Party Software Updates + OS Updates **Patch Strategy** configures how updates for Windows and Apple machines are performed on assigned machines. Additionally, it allows to use 3rd party software management.

- All agents assigned a **Scan and Analysis** profile using the Third-Party Software Updates + OS Updates patch strategy must have a **Deployment** profile assigned to them or 3rd-party software patches will not be deployed.
- The schedule section governs only scans of 3rd-party software. It is not related to OS updates configuration defined in the sections below which are applied immediately. At the times specified in the schedule every endpoint assigned to the profile is scanned. The scan checks if software defined in 3rd-Party Software profile is installed and up to date.
- OS updates configuration sections are described in detail in **Only OS Updates** section

Software Management > Profiles > Scan and Analysis

A profile using the CloudActiv8 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 or the **Machines** page.

- All agents assigned a **Scan and Analysis** profile using the CloudActiv8 Update patch strategy must have a **Deployment** profile assigned to them **or patches will not be deployed.**
- 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** or **3rd-Party Software** profile. Overrides are assigned to machines using the **Assign Profiles** button on the **Machines** 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, 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.
  - **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. Software titles are deployed based on the schedule specified by a machine's assigned **Deployment** 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.

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.

- **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 (re-ask 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 xxii)* 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.

Note: If patch deployments configured with **Reboot immediately after update** happen to complete within any blackout window, reboots will be suspended until the next scheduled deployment window.

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 vi)* scan by at least several hours.

- **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 CloudActiv8 users. Alerts are processed every six hours.

Reviewing Alarms Created by Software Management Alerts

- Monitor > **Alarm Summary**
- Monitor > Dashboard List > any **Alarm Summary Window** within a dash let
- Agent > Agent Logs > **Agent Log**
- The Agent > Agent Logs > **Monitor Action Log** - Shows the actions taken in response to an alert, whether or not an alarm was created.
- **Live Connect** > Asset > Log Viewer > Alarm

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.
- **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** profile. Specifies the **Subject** and **Body** format of email notifications that a machine needs to be rebooted after a patch.
  - **Compliance** - Compliance checking is reported on the **Dashboard** page and in Info Center > **Report Parts** for **Software Management**.
    - ✓ **Compliance Check** - Specifies how often machines are checked for compliance, based on CloudActiv8 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.
  - **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
  - **Private Profiles** - If checked, profiles are only visible if the profile was created by you or if the profile is assigned to a machine assigned to the scope you are using. Profiles are public by default. Applies to the following types of profiles:
    - ✓ Scan and analysis
    - ✓ Override
    - ✓ 3rd Party Software
    - ✓ Deployment
    - ✓ Alerting
  - **Ignore 3rd-Party Patches** - If checked, 3rd party patches are not included in scans and deployments.

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** page. The migration creates a new **KB override profile** in **Software Management** with the name you specify.

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**. Optionally migrates machine associations. This migration creates a new **KB override profile** 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.