Seqrite Endpoint Security 8.1

Patch Management Guide

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Patch Management

Patch Management (PM) enables centralized management for checking and installing the missing patches for the applications installed in your network. With this, you can also automate the checking and installation of the missing patches. Patch Management helps to identify endpoints integrity (host integrity) and reflects the status of the compliance in the reports.

Workflow of Patch Management

1. Install the Patch Management server
2. Add Patch Management server
3. Configure the Patch Management server
4. Scan for missing patches
5. Select the missing patches and install the patches
6. Generate a report of the installed missing patches

System Requirements

System requirements for the Patch Management server are as follows:

Component	Requirements
Processor	4 Core(x86-64) and above
RAM	8 GB or more
Hard disk space	Minimum: 40 GB free disk space Recommended: 1 TB free disk space
Display	1024 x 768
OS	• Microsoft Windows 10 (64-bit) and above • Microsoft Windows Server 2012 (64-bit) and above
	• For more than 25 clients, Seqrite recommends to install a Patch Management server on the Windows Server operating system.

Recommendation

For the remote clients, install the Patch Server in the network where the remote clients are deployed. The private IP of the Patch server should be natted to the public IP.

Adding Patch Server

Adding patch server

Prerequisite

If you are adding the patch server by Hostname, you need to add the hostname and IP address, manually in the 'hosts' file located in the 'etc' folder.

To add a patch server, follow these steps.

1. Go to **Computer** > **Configurations** > **Patch Management**.
2. Click the Download Patch Server Setup button to download the setup file.
3. Follow the steps displayed on the UI to proceed.
4. Click **Add Patch Server**. The Add Patch Server dialog appears.
5. Enter the patch server name.
6. Enter the patch server IP/ Hostname.
7. Enter the SSL Port number.
8. Enter the EPS server IP/ Hostname.
9. After entering these details, click **Add**.

   The new patch server is added now and appears on the Patch Management page.

Editing patch server

To edit a patch server, follow these steps.

1. Go to **Computer** > **Configurations** > **Patch Management**. Existing patch servers are listed.
2. Click the Edit icon of the patch server that you want to edit.
3. The patch server details appear. In Patch Synchronization and Configuration tab, you can view the previous patch synchronization status with a time stamp.
4. Here you can edit the SSL port number. Also, you can edit the Patch Synchronization details, as required.
5. In the Internet Settings tab, change proxy settings if required.
6. Click **Save.**

Applying filters

If you select the Parent patch server as Microsoft, then only these filters are applicable.

If you select the Parent patch server as WSUS, all metadata available on WSUS is synchronized. Microsoft filters are not applicable.

To apply filters, follow these steps.

1. If you want to apply filters for downloading and synchronizing the patches, click **Apply Filters**.
2. The Filters dialog appears.
3. In **Categories** accordion, click + to expand. Either you can select the **All Categories** check box to select all categories to be synchronized for Microsoft applications or select the type of patches from the list, as required.
4. In **Languages** accordion, click + to expand.
5. Here you can select the languages for the patches for Microsoft applications. Select one of the following options.
   - Download patches in all languages
   - Download patches in the following selected languages – If you select this option, select the languages from the list.
6. In the **Products** accordion, click + to expand.
7. Here you can select the products for which you want to receive the patches. Either you select All products or select products as required from the list.
8. Click **Apply**.

   The patch settings are updated.

When the patch synchronization is complete as per the applied filters, the patch synchronization status is shown as **Successful** with the timestamp.

When the patch synchronization is failed as per applied filters, the patch synchronization status is shown as **Failed** with the timestamp.

Deleting patch server

To delete a patch server, follow these steps.

1. Go to **Computer** > **Configurations** > **Patch Management**. Existing patch servers are listed.
2. Click the **Trash** icon of the patch server that you want to edit.
3. Click **Yes** on the confirmation dialog box.

   The patch server is deleted.

Patch Scan Policies

This feature allows you to configure a patch server for the policies in the network. This helps to install the missing patches on the endpoints.

To configure the patch server, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Policies**. Click the Edit icon next to the policy for which you want to configure the patch server.
3. Under Policy Settings, click **Patch Server**.
4. Switch the Configure Patch Server toggle button to turn it on.

   Expand this section by clicking the Expand icon.
5. From the drop-down menu, select the patch server to scan.
6. Select the **Use Microsoft patch…..roaming endpoints** check box if required.
7. Click **Save Policy**.

   A success dialog appears.

Performing Patch Scan

This feature allows you to scan the missing patches on the selected endpoints in the network.

To initiate scanning of the missing patches, follow these steps:

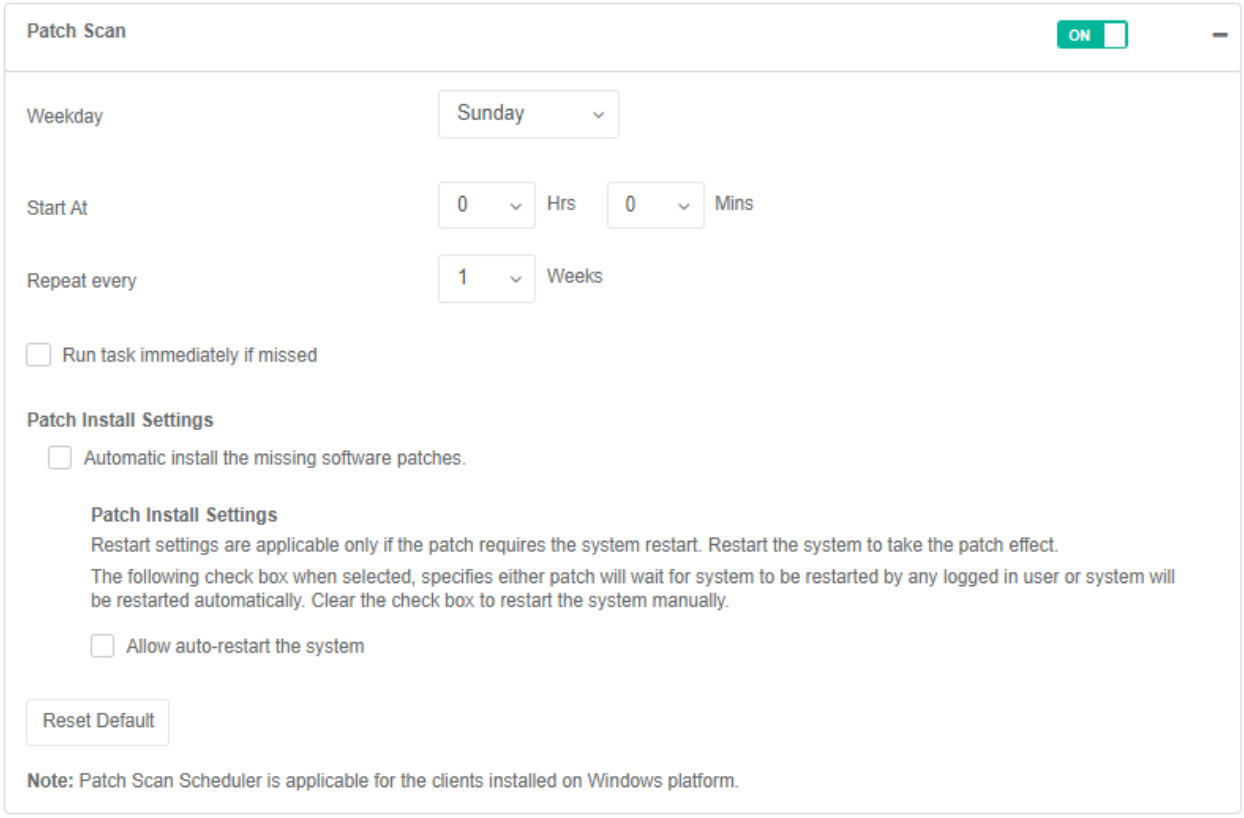
1. Log on to the Seqrite Endpoint Security Web console.

   Go to **Computer** > **Status**.
2. On the Status page, select the endpoints you want to scan.
3. The client action bar is enabled above the table. In the Client Actions drop-down, select **Patch Scan**.
4. In the Please Select drop-down menu, select **Start Scan**.
5. Click **Submit**.

   You can stop scanning by clicking **Stop Scan** at any time you prefer.

Configuring Schedule for Patch Scan

This feature allows you to configure a schedule for scanning missing patches.



To configure a patch scan schedule, follow these steps.

1. Select a weekday from the drop-down menu.
2. In **Start At**, set the time in hours and minutes.
3. If you want to repeat the scanning of your clients, set the frequency to repeat the scan in weeks.
4. Select the **Run task immediately if missed** checkbox if you want to run the scan if missed the set schedule.
5. Under Patch Install Settings, select the **Automatic install the missing software patches** check box if required.

   Note: Automatic Install feature is not applicable for roaming endpoints.
6. Select the **Allow auto-restart the system** check box if required.

Installing Missing Patches

This feature allows you to install the missing patches on the selected endpoints.

To install the missing patches, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.

   Go to **Computer** > **Status**. Click **Patch Install**.

   Patch Install page appears. A list of the missing patches appears.

2. You can filter the list with the help of the four filters described in the following tables:

   Severity options:

Severity	**Description**
Critical	The vulnerability may allow code execution without user interaction.
Important	The vulnerability may result in the compromise of the confidentiality, integrity, or availability of user data. The client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability.
Moderate	The impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low	The impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Unspecified	The vulnerability may result in random malfunctions.

   Category options:

Category	Description
Security Updates	A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low.
Update Rollups	A tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a component of a product, such as Internet Information Services (IIS).

Applications	Application (software) is a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform.
Service Packs	A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.
Feature Packs	New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.
Updates	Updates are code fixes for products that are provided to individual customers when those customers experience critical problems for which no feasible workaround is available.
Definition Updates	A widely released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects that have specific attributes, such as malicious code, phishing websites, or junk mail.
Critical Updates	A widely released fix for a specific problem that addresses a critical, non-security-related bug.

Restart Required options:

Restart Required	**Description**
All	Display result for all the options.
Not Required	The patch does not require a system restart.
Required	The patch requires the system restart. Restart the system to take the patch effect.
May Require	The patch may require a system restart.

EULA Status options:

EULA Status	**Description**
All	Display the result for both the options, Accepted and Not Accepted.
Accepted	The end User License Agreement is accepted.
Not Accepted	End User License Agreement is not accepted.

3. To generate the result with help of filters and/or record details, click **Generate Report**.
4. Select the **Show patches within the subgroup** check box to display the name of the patches that are in the subgroup from the list of the endpoints without actually exploring the network.
5. To change the restart setting, click the **System Restart Settings** button. Restart settings are applicable only if the patch requires the system restart.
6. Select the **Allow auto-restart the system** check box to restart the system automatically. Clear the check box to restart the system manually.
7. From the missing patches list, select the patches that you want to install.
    a. Click the patch name.

       The Patch Details dialog appears.

    b. In the list, click the number in the column **No. of Endpoint Affected**. Endpoint(s) affected dialog appears.

       Select the endpoints where you want to install the missing patch.

       Click **Apply**. The list of endpoints is saved.

       The count in the column **No. of Endpoint selected** is updated.
8. Click **Start Install**. To cancel the selection, click **Refresh.**

Patch Management report

You can view reports of the installed/missing patches on the endpoints in the network. In the Patch Management report, you can view the name of the patch in the hyperlink format. You can click the name to view the details of the patch.

This report is only in the tabular format, not in the chart format.

Patch Information on Dashboard

The dashboard page has widgets for the following information about patch management.

Feature	Description
Number of missing patches by severity	Displays the number of missing patches according to their severity (critical, important, moderate, low, and unspecified) in the form of a bar chart.
Patch scan overview	Displays the information for the patch scans. The count of endpoints with missing patches, endpoints not scanned, and Up-to-Date endpoints are displayed.