Thirtyseven4 EDR Security

Patch Management Guide

Thirtyseven4, LLC.

www.thirtyseven4.com

Release Date

April 10, 2024

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.

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, Thirtyseven4 recommends installing a Patch Management server on the Windows Server operating system.

Note: The machine on which you are installing the Patch Management Server must be on the Public IP network.

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

Installing Patch Management Server

To begin installation of Patch Management server, follow these steps:

Note: The machine on which you are installing the Patch Management Server has to be on the Public IP network.

1. For 64-Bit Windows OS, download the setup from one of the following links:

   https://dlupdate.quickheal.com/builds/seqrite/uemcp/pms/en/pmsetup64.msi

   https://download.quickheal.com/builds/seqrite/uemcp/pms/en/pmsetup64.msi

2. Launch the setup on machine within the network where you want to install the Thirtyseven4 patch server. The Thirtyseven4 Patch Management Server Setup Wizard screen appears.
3. On the Patch Management Server Setup Wizard, click **Next**. The license agreement appears. Read the License Agreement carefully.
4. Select the **I Agree** check box to accept the license agreement and then click **Next**.
5. It asks for the installation location. Click **Browse** if you want to install Patch Management server on a location different than the default location. To proceed with the default installation path, click **Next**.
6. The **Patch Database Settings** screen appears. The patch content storage folder path appears. Click **Browse** if you want to change the patch content storage path.
7. Select the **Import Patch Server Data** check box if you want to change the default location. Click **Browse** to locate the path.
8. Click **Next**.
9. The **Proxy Settings** screen appears. To enable and configure proxy settings, do the following:
   a. Select the **Enable Proxy Settings** check box.
   b. In the **Proxy Server** text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).
   c. In **Port** text box, type the port number of the proxy server (For example: 80).
   d. Select the **Enable Authentication** (If any) check box.
   e. In the Username and Password fields, type in your server credentials.
   f. Click **Next**.
10. The **MySQL 5.7.37 Location** screen appears.

You need to provide a path for MySQL 5.7.37 setup file.

If you do not have MySQL 5.7.37 setup file, download it from the given link and provide the path.

11. Click **Next**. The file will be verified.
12. The **MySQL Configuration Setting** screen appears.
    a. Enter **Communication Port** number.
    b. Enter password for MySQL 'Root' user. In the Confirm password text box, retype the password.
    c. Click **Next**.
13. In the **Upstream Patch Server** screen, select one of the following:
    - Microsoft: The upstream patch server used is Microsoft patch server. This option is selected by default.
    - Organization Patch Server (WSUS): The upstream patch server used is Organization Patch server (WSUS – Windows Server Update Service). If you select this option, type in WSUS server URL.
14. Click **Next**.
15. On the Website Configuration page,
    a. Click the Public IP radio button. Enter the Public IP.
    b. In the SSL Port text box, enter the SSL port number. This port number will serve as a listening port for the server.
    c. Click **Next**.
16. On confirmation prompt, click **Yes**.
17. The installation summary screen appears. You can change the settings if required by clicking **Back**.

    Click **Install**. The installation starts.

    It might take a few minutes to complete the installation. The wizard shows **Installation in Progress.** Once the installation is successfully done, the following screen appears.
18. To complete the installation, click **Finish**.

    If installation/uninstallation fails, then only the View installation log check box is displayed. To view the log, select the View installation log check box.
19. After the installation is complete, add Thirtyseven4 patch server through EPP console and then it becomes available to use.

The Patch Management feature is applicable only for clients with Microsoft Windows OS; it does not support Mac, and Linux operating systems.

Back up the Patch Server Data

You can back up the patch database and patch content of the patch server.

To back up the patch server data, follow these steps:

1. Manually back up all the files and folders present in the /Thirtyseven4 patch management/patch server/content folder.
2. Select **Start** > **Programs** > **Thirtyseven4 Patch server Data Backup**.

   The Backup wizard starts.
3. Click **Browse** to specify the path where you want to back up patch database.
4. Click **Backup**.

The database file, **pmdb.exp** is generated. This file can be used to restore patch server database.

Uninstalling Patch Server

If you need to uninstall the patch server, follow these steps:

1. Go to **Start** > **Programs** > **Uninstall patch server**.

   The uninstaller wizard starts.
2. Complete the wizard to uninstall the 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 of the machine on which patch server is installed.

To add a patch server, follow these steps.

1. Go to the console > **Configurations** > **Patch Management**.
2. Click the Download Patch Server Installer 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 **Public IP/Hostname** of the system where Patch Server is installed.
7. Enter the SSL Port number. By default 6201 appears.
8. After entering these details, click **Add**.

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

   You can add multiple Patch Servers.

   If multiple patch servers are added, you can sort the list as per Patch Server Name, Patch Server IP/Hostname, and Status.

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. By default, the Upstream Server is Microsoft Patch Server. You can change the Upstream Patch Server if required. If you select the option **Local Thirtyseven4 Patch Server**, select the server from the list.
6. In the Internet Settings tab, change proxy settings if required.
7. Click **Save.**

Schedule Patch Synchronization

1. Select the **Enable Schedule Patch Synchronization** check box.
2. Select the Frequency of patch synchronization, either **Weekly** or **Monthly**.
3. Select **Weekday** from the list to run patch synchronization.
4. Select the time to run patch synchronization by selecting hours and minutes in the **Start At** list.
5. Click **Apply Filters** to specify filters for patch synchronization.
6. Click **Start sync** to run patch synchronization instantly.
7. You can click **Stop sync** to stop patch synchronization if it is running. A notification is sent to the patch management server.

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.

If you select the Upstream Patch Server as Local Thirtyseven4 Patch Server, then filters enabled on the selected server are applicable.

To apply filters, follow these steps.

1. If you want to apply filters for downloading and synchronizing the patches, click **Apply Filters**. The Filters dialog appears.
2. 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.
3. In **Languages** accordion, click + to expand.

   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.
4. In the **Products** accordion, click + to expand.

   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.
5. Click **Apply**.

   The patch settings are updated.

Patch Management supports the following applications along with Microsoft applications,

- Adobe
- VideoLAN
- Adobe Systems, Inc.
- Microsoft
- PuTTY
- Notepad++, Inc.
- Oracle Corp.
- 7-Zip

- Mozilla Foundation

Patch Synchronization

To start patch synchronization, follow these steps.

1. Go to Patch Server Task Scheduler > Task Scheduler Library.
2. Run Thirtyseven4 Schedule Patch Sync to trigger on demand Patch Sync.

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 Thirtyseven4 EDR 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 Thirtyseven4 EDR 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 Thirtyseven4 EDR Security Web console.

   Go to the console > **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.