29 July 2019

CHECK POINT ENDPOINT SECURITY
R77.30 - EP6.5
Limited Customer Release

Release Notes
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Check Point R77.30 - EP6.5
For more about this release, see the R77.30 - EP6.5 home page http://supportcontent.checkpoint.com/solutions?id=sk117512.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=55665.
To learn more, visit the Check Point Support Center https://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point Endpoint Security R77.30 - EP6.5 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 July 2019</td>
<td>Updated release of this document for the Offline Tool System Requirements</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>What’s New</td>
<td>6</td>
</tr>
<tr>
<td>Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Offline Management Tool System Requirements</td>
<td>7</td>
</tr>
<tr>
<td>Installation and Upgrade</td>
<td>7</td>
</tr>
<tr>
<td>Installing on R77.30</td>
<td>7</td>
</tr>
<tr>
<td>Advanced Upgrade from Earlier EP Release</td>
<td>8</td>
</tr>
<tr>
<td>Installing the SmartConsole</td>
<td>9</td>
</tr>
<tr>
<td>Upgrading with Online Synchronization</td>
<td>9</td>
</tr>
<tr>
<td>Java Upgrades</td>
<td>10</td>
</tr>
<tr>
<td>Media Encryption Features</td>
<td>10</td>
</tr>
<tr>
<td>Configuring Encryption Container Settings</td>
<td>10</td>
</tr>
<tr>
<td>Migrating Media Encryption Remote Help Keys from R73 Servers</td>
<td>11</td>
</tr>
<tr>
<td>Full Disk Encryption Features</td>
<td>11</td>
</tr>
<tr>
<td>Self-Help Portal</td>
<td>11</td>
</tr>
<tr>
<td>Activating the Self-Help Portal</td>
<td>11</td>
</tr>
<tr>
<td>Configuring the Self-Help Portal</td>
<td>12</td>
</tr>
<tr>
<td>User Settings for the Self-Help Portal</td>
<td>13</td>
</tr>
<tr>
<td>Monitoring the Self-Help Portal</td>
<td>13</td>
</tr>
<tr>
<td>Temporary Pre-boot Bypass</td>
<td>13</td>
</tr>
<tr>
<td>Temporary Pre-boot Bypass with LAN</td>
<td>14</td>
</tr>
<tr>
<td>Changing the Volume Encryption Algorithm</td>
<td>14</td>
</tr>
<tr>
<td>Creating and Managing Pre-boot Users</td>
<td>15</td>
</tr>
<tr>
<td>In-place Re-imaging</td>
<td>17</td>
</tr>
<tr>
<td>AD Groups for Pre-boot Authentication</td>
<td>18</td>
</tr>
<tr>
<td>Managing Authorized Pre-boot Users and Nodes</td>
<td>19</td>
</tr>
<tr>
<td>User-Bound Remote Help</td>
<td>20</td>
</tr>
<tr>
<td>Offline Mode</td>
<td>21</td>
</tr>
<tr>
<td>Creating Offline Administrators</td>
<td>21</td>
</tr>
<tr>
<td>Configuring an Offline Group</td>
<td>22</td>
</tr>
<tr>
<td>Configuring Policy for an Offline Group</td>
<td>23</td>
</tr>
<tr>
<td>Editing Pre-boot Users</td>
<td>24</td>
</tr>
<tr>
<td>Exporting Packages</td>
<td>25</td>
</tr>
<tr>
<td>Deploying Packages</td>
<td>26</td>
</tr>
<tr>
<td>Moving from Offline to Online Mode</td>
<td>27</td>
</tr>
<tr>
<td>Endpoint Offline Management Tool</td>
<td>27</td>
</tr>
<tr>
<td>Logging In to the Offline Tool</td>
<td>28</td>
</tr>
<tr>
<td>Password Recovery</td>
<td>28</td>
</tr>
<tr>
<td>Disk Recovery</td>
<td>29</td>
</tr>
<tr>
<td>Encryption and Certificate Features</td>
<td>30</td>
</tr>
<tr>
<td>External PKI Certificates</td>
<td>30</td>
</tr>
<tr>
<td>Importing Certificates</td>
<td>30</td>
</tr>
<tr>
<td>Installing CA Certificates on Clients</td>
<td>31</td>
</tr>
<tr>
<td>Installing SSL Certificates on Servers</td>
<td>31</td>
</tr>
<tr>
<td>Replacing SSL Certificates in an Existing Environment</td>
<td>32</td>
</tr>
</tbody>
</table>
Introduction

Thank you for installing Check Point Endpoint Security R77.30 - EP6.5. This release includes a new Endpoint Security Management Server on top of R77.30 and a new SmartConsole.

What's New

New in this release:

- Improved scaling and response times to Full Disk Encryption client messages.
- Directory Scanner initial scan and full re-scan take significantly less time.
- Stability and performance enhancements for Online Automatic Synchronization [High Availability].
- Support for new Full Disk Encryption algorithms, XTS-AES 128-bit and XTS-AES 256-bit for UEFI systems.
- General performance improvements.

Requirements

Server Requirements

- This release is supported on Gaia operating system only.
- Install R77.30 - EP6.5 as a hotfix on top of R77.30 or as an advanced upgrade from R77.20 EP6.0 or R77.20 EP6.1.

Endpoint Security Client Requirements

Only Media Encryption and Full Disk Encryption blades are supported in this version. R77.30 - EP6.5 servers can manage:

- Endpoint Security Windows clients - E80.70 and E80.51 EP6.0
- Endpoint Security Mac clients - E80.64 and E80.62

For additional requirements, see the Release Notes document for your client version.
Offline Management Tool System Requirements

Minimum hardware requirements:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>1 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB</td>
</tr>
<tr>
<td>Disk space</td>
<td>32-bit: 1 GB</td>
</tr>
<tr>
<td></td>
<td>64-bit: 2.5 GB</td>
</tr>
</tbody>
</table>

Software requirements:
- Microsoft Visual C++
  - Offline Management Tool E80.92 and higher require MSVCR 2017
    - **Note** - Formerly, all other versions (prior to Offline Management Tool E80.92) required MSVCR 2008 and 2012
- .NET framework 4.5
- OS: Windows 7, 8.1, 10 - 32 and 64-bit

Installation and Upgrade


Installing on R77.30

Install R77.30 - EP6.5 as a hotfix on top of R77.30.

**To install an R77.30 - EP6.5 Endpoint Security Management Server:**

1. Install an R77.30 Security Management Server or upgrade to R77.30. Use the procedures in the [R77.30 Release Notes](http://downloads.checkpoint.com/dc/download.htm?ID=40107).
   Or use an existing R77.30 installation.
2. Back up your R77.30 Security Management Server.
3. Create a temporary directory.
5. Save the file to a temporary directory.
6. Connect to the management server with SSH.
7. Run these commands in expert mode:
   - `tar -zxvf <filename>.tgz`
   - `./UnixInstallScript`
8. Reboot.

**Best Practice** - If you have Java 32-bit, upgrade to Java 64-bit [on page 10].
Advanced Upgrade from Earlier EP Release

Perform an Advanced Upgrade from an existing R77.20 EP6.0 or R77.20 EP6.1 server to a new, clean Endpoint Security Management Server on Gaia. Export the Endpoint Security database from the existing server and import it to the new server.

In an environment with High Availability, Endpoint Policy Servers, or Remote Help Servers:

1. After you complete the Advanced Upgrade of the primary Endpoint Security Management Server, you must install other servers as new installations and connect and synchronize them with the primary Endpoint Security Management Server. Use the instructions in the Endpoint Security Administration Guide.
2. In SmartDashboard, make sure that you delete server objects from the old installation and create new objects for new servers.

If you have multiple Endpoint Security servers in an environment, follow the upgrade procedure for all servers.

To upgrade to R77.30 - EP6.5 with Advanced Upgrade:

1. Install a new R77.30 - EP6.5 Endpoint Security Management Server as described in Installing on R77.30 (on page ?).
2. Get Migrate Tools from the home page.
3. Extract the files to a temporary folder on the existing Endpoint Security Management Server.
4. Export the database from the existing Endpoint Security Management Server.
   
   `<filename>` is a name that you choose for the .tgz file.
   
   - To automatically include all client MSI packages, run:
     
     ```
     ./migrate export --include-uepm-msi-files <filename>.tgz
     ```
   
   - To export files without MSI packages, run:
     
     ```
     ./migrate export <filename>.tgz
     ```

5. Copy the TGZ file to the new R77.30 - EP6.5 Endpoint Security Management Server that you created.
6. On the new R77.30 - EP6.5 Endpoint Security Management Server, use the local migrate tools [`$FWDIR/bin/upgrade_tools`] to run one of these commands.

   `<filename>` is the name of the .tgz file, as you entered it during the export.

   - To automatically include all client MSI packages, run:
     
     ```
     $FWDIR/bin/upgrade_tools/migrate import --include-uepm-msi-files <filename>.tgz
     ```
   
   - To import files without MSI packages, run:
     
     ```
     $FWDIR/bin/upgrade_tools/migrate import <filename>.tgz
     ```
7. If you did not export and import the MSI packages to the new server in the previous steps, copy them manually:
   a) Copy $FWDIR/conf/SMC_Files/uepm/msi from the source server to the same location on the target server.
   b) On the target server, change the permissions for the MSI folders. Run:
      (i) cd $FWDIR/conf/SMC_Files/uepm
      (ii) chmod -R u+rwx,g+rwx,o-rwx msi/
      (iii) find msi/ -type d -exec chmod g+s {} \
   c) Make sure that the permissions were changed correctly.

Installing the SmartConsole

To install the SmartConsole for this version:
Download the SmartConsole from the home page and run it.

Note - If you have another version of R77.30 SmartConsole installed on your computer, you must first uninstall it, and then install the R77.30 - EP6.5 SmartConsole.

Upgrading with Online Synchronization

To upgrade to this release in an environment that uses online synchronization:
1. On each Endpoint Security Management Server (including secondary servers), and Remote Help Server, run:
   /opt/CPshrd-R77/bin/PgOnlineSyncUtil stop_engine
   Note - Do not run this on Endpoint Policy Servers.
2. Upgrade the primary server (active). Wait for the upgrade to finish.
3. Upgrade the secondary server. Wait for the upgrade to finish.
5. Upgrade Endpoint Policy Servers. You can do this while other servers are upgrading.
6. Online synchronization engines are reconfigured during the upgrade, so synchronization starts among all servers. Do these steps to make sure the sync worked as expected:
   a) Run: PgOnlineSyncUtil is_initial_load_over on the secondary and Remote Help Servers and make sure they are finished.
   b) Check the Management High Availability state in SmartDashboard. Make sure that the state is Synchronized with no error.
Java Upgrades

By default, Endpoint Security Server installed on Gaia OS runs Java 32-bit. Endpoint Security Server also supports Java 64-bit, which provides better performance for systems with RAM size equal to or larger than 4GB.

To use an Endpoint Security Server in 64-bit mode, you must configure Gaia OS to automatically boot to the 64-bit kernel edition and upgrade Java to 64-bit.

**To use an Endpoint Security Server in 64-bit mode:**

1. Connect to command line on Gaia OS.
2. Log in to clish.
   
   Run: `set edition 64-bit`
4. Save the Gaia Database.
   
   Run: `save config`
5. Reboot the computer.
6. Make sure that the Gaia OS booted with the 64-bit kernel edition.
   
   Run: `show version all`

**To upgrade to Java 64-bit:**

Run: `$UEPMDIR/system/utils/replace_ibm_jre_to_64_bit`

**To revert to Java 32-bit:**

Run: `$UEPMDIR/system/utils/replace_ibm_jre_to_64_bit uninstall`

---

Media Encryption Features

Configuring Encryption Container Settings

In this release, you can configure options for setting the encrypted space on storage devices.

**To configure encryption settings for users on storage devices:**

1. In the SmartEndpoint **Policy** tab, select a **Media Encryption & Port Protection** rule.
2. Clone the **Offline access to encrypted storage devices** action.
3. In the cloned action, under **Allow offline access to encrypted storage devices**, select **Allow user to change the size of encrypted media**.
4. Set the **Minimum percentage** and **Default percentage** of **free space** - how much of the device’s free space can be used.
   
   Or set the **Minimum percentage** and **Default percentage** of **media capacity** - how much of the device’s total capacity can be used.

**To force encryption of all media:**

1. Do not select **Allow user to change the size of encrypted media**.
2. Set the **Minimum percentage** and **Default percentage** of **media capacity** to 100.
Migrating Media Encryption Remote Help Keys from R73 Servers

To migrate all Media Encryption Remote Help keys from R73 to this version:

1. In SmartEndpoint, go to Tools > Devices and Keys Migration Tool.
   The Devices and Keys Migrator wizard opens.
2. Enter SQL server details.
3. Click Next.
4. Make sure Import WebRH Keys is selected.
5. Click Next.
7. Click Finish.

Full Disk Encryption Features

Self-Help Portal

The Self-Help Portal (SHP) adds Full Disk Encryption functionality to let users reset their own passwords autonomously. To use the Self-Help Portal, the user must register to the portal first. After registration users can use the Self-Help Portal for password recovery.

The portal is available for desktop and mobile devices.

These browsers and devices are supported:

Mobile:
- Google Chrome 41 or higher (Android 4 or higher)
- Android Browser (Android 4 or higher)
- Safari (iOS 6.1.3 or higher)

Desktop:
- Internet Explorer 9-11
- Mozilla Firefox 36.0.1 or higher
- Google Chrome 41 or higher

Activating the Self-Help Portal

You must enable the Self-Help Portal on the Endpoint Security Management Server to activate it.

Note - On the Gaia portal > Hosts and DNS page, make sure to configure:
- The DNS Server
- Domain Name
- DNS suffix
To enable the Self-Help Portal:
On the Endpoint Security Management Server, run:
```bash
cd $UEPMDIR/engine/jre/bin/
selfhelp_cmd enable
```
Note that this restarts the Endpoint Security Management Server.
After activation, the Self-Help Portal is available at `http://<eps_server_ip>/eps_shp`
where `<eps_server_ip>` is the IP address of the Endpoint Security Management Server.

To disable the Self-Help Portal, run:
```bash
selfhelp_cmd disable
```

To query the status the Self-Help Portal, run:
```bash
selfhelp_cmd status
```

Configuring the Self-Help Portal
The Self-Help Portal only works with Active Directory users. Before you can use the Portal, make sure that the Endpoint Security Active Directory Scanner is configured and that the Active Directory is scanned.

Users must be authorized for Pre-boot on one or more computers before they register in the Portal.

To configure Self-Help Portal settings in SmartEndpoint:
1. In the Policy Tab, in a User Authentication (OneCheck) rule, right-click the Allow password self help action and select Edit.
2. Select Allow password self-help to let users recover their password by answering questions. Clear the option to not let users recover their password by answering questions.
3. Make selections to configure the options for Enrollment to the Portal and for Password Assistance.
4. Click Questions Bank to select which questions are asked for user enrollment to the Self-Help Portal.
5. Click OK.
6. Click OK.
7. Save.
8. Click Install Policy and select the Self-Help Settings Policy.

Users can register to the Self-Help Portal and use it to recover passwords. The portal address is `http://<eps_server_ip>/eps_shp`
where `<eps_server_ip>` is the IP address of the Endpoint Security Management Server.
**User Settings for the Self-Help Portal**

You can force users to re-register to the Self-Help Portal or block users from recovering passwords in the portal.

**To change a user’s settings for the Self-Help Portal:**

1. In SmartEndpoint, in the **Users and Computers** tab, right-click on a user and select **User Authentication policy**.
2. Select **Reset Self-Help Enrollment** to force the user to re-register to the portal.  
   Select **Lock Password Self-Help** to prevent users from recovering passwords in the portal.

**Monitoring the Self-Help Portal Policy**

**To see the status of user enrollment and recovery for the Self-Help Portal:**

In SmartEndpoint, in the **Reporting** tab, select **User Authentication Policy > Self Help Status**.

**Temporary Pre-boot Bypass**

There are different types of policy configuration for Temporary Pre-boot Bypass:

- Temporary Pre-boot Bypass
- Temporary Pre-boot Bypass with script
- Temporary Pre-boot Bypass with LAN (on page 14)

Temporary Pre-boot Bypass and Temporary Pre-boot Bypass with script are part of Full Disk Encryption. The device key is temporarily stored on the disk with low protection. When Full Disk Encryption Pre-boot starts and

- there is no user input
- the device key is available

Full Disk Encryption cancels the user authentication and starts the OS.

Endpoint Security Management Server cannot receive policy updates when offline. Set to enable or disable Temporary Pre-boot Bypass when online for future use.

Use **New policy configuration settings** to set the start time, expiration, and optional repeat interval. Full Disk Encryption automatically creates or removes the temporary storage of the device key on the disk.

In Temporary Pre-boot Bypass with script, the schedule configuration is the time period that Full Disk Encryption allows the user to enable the Temporary Pre-boot Bypass and run the script (FDEcontrol.exe).

**Note** - In the **Users and Computers** tab, enable the action button to disable or revert the Pre-boot action. Full Disk Encryption enforces these actions when Temporary Pre-boot Bypass is enabled and the current time is not outside the schedule.
Temporary Pre-boot Bypass with LAN

Temporary Pre-boot Bypass when connected to LAN lets you set upgrades to install or do maintenance when computers are turned off. The updates happen automatically after the computers are turned back on. The administrator configures Temporary Pre-boot Bypass for the required time and makes sure that Allow bypass when connected to LAN is selected.

Make sure that you have the Unlock on LAN Requirements shown in the R77 Release Notes http://supportcontent.checkpoint.com/documentation_download?ID=24827.

To manage the bypass feature, the Pre-boot must be disabled or enabled from the Users & Computers tab.

To configure Temporary Pre-boot Bypass when connected to LAN:

1. In the SmartEndpoint Policy tab, in a Full Disk Encryption rule, click Authenticate user before OS loads (enable Pre-boot).
2. Click OK.
   The Temporary Pre-boot Bypass Settings window opens.
3. In Schedule Temporary Pre-boot bypass to specific time interval, select Allow Pre-boot bypass (Wake On LAN - WOL).
   You can select Allow Bypass Script for other options.
4. Click OK.
   A new window opens.
5. Select a Bypass period for Temporary Pre-boot Bypass: If the bypass period occurs Once or Weekly.
   • If you select Weekly:
     ▪ Day of week - The day of the week for the bypass.
     ▪ Bypass start hour - When the bypass starts.
   • If you select Once:
     ▪ Bypass start date - The date the bypass will start.
     ▪ Bypass start time - The time the bypass will start.
6. Select the Temporary Pre-boot Bypass Duration (configure one or both options)
   • Disable after X Automatic logons - Select this to turn off the bypass after the configured number of logins to a computer.
   • Disable after X Days - Select this to turn off the bypass after the configured amount of time passed.
7. Click OK.

Changing the Volume Encryption Algorithm

In the Disk Encryption action, you can change the volume encryption algorithm. These algorithms are newly added:

• XTS-AES (256-bit)
• XTS-AES (128-bit)

Note - These are only available for UEFI-systems. Best practice is not to use this in environments with both UEFI and BIOS systems, as BIOS systems will default back to AES-CBC.
Creating and Managing Pre-boot Users

There are two types of pre-boot users:

- Online
- Offline

Creating Online Preboot users

Preboot users can be assigned or not assigned to a node.

To create new online Pre-boot user assigned to a node:

1. Open SmartEndpoint Manager.
2. On the Users and Computers tab, right-click on an OU under Directories or Other Users/Computers.
4. Click New.
   The Add new Preboot user window opens.
5. Enter a Logon Name
6. In the Authentication credentials area, select Password or Dynamic Token.
   - A password must contain at least five characters
   - If you select a token as the authentication method, make sure you select an existing token
7. To set more granular account controls, open Account Details.
   - Do not use device information for Full Disk Encryption remote help - Enables user-bound remote help for the pre-boot user
   - Lock user for preboot - Locks the user for preboot
   - Require change password after first logon - Applies only to password authentication. Select this option to force users to change their password after the first pre-boot logon.

8. To set an account expiration date, open the Expiration Settings.
   a) Select The user will be revoked after option.
   b) Select a date.
   Note - the default expiration setting is: Never

To create a preboot user not assigned to a node:

   The Add new preboot user window opens.
2. Enter a Logon Name
3. In the Authentication credentials area, select Password or Dynamic Token.
   - A password must contain at least five characters
   - If you select a token as the authentication method, make sure you select an existing token
4. To set more granular account controls, open Account Details.
   - Do not use device information for Full Disk Encryption remote help - Enables user-bound remote help for the pre-boot user
   - Lock user for preboot - Locks the user for preboot
• **Require change password after first logon** - Applies only to password authentication. Select this option to force users to change their password after the first pre-boot logon.

5. To set an account expiration date, open the **Expiration Settings**.
   a) Select **The user will be revoked after** option
   b) Select a date

**Creating Offline Preboot users**
1. Open **Smart Endpoint Manager**.
2. On the **Users and Computers** tab, select an offline group.
3. In **Group Details**, click **Edit**.
   The **Group Details** window opens.
4. Click **Pre-boot Users**.
   The **Pre-boot Users Details** window opens.
5. In the **Authorized Preboot Users** area, click **New**.
   The **Add new preboot user** window opens.
6. Enter a **Logon Name**
7. In the **Authentication credentials** area, select **Password** or Dynamic **Token**.
   • A password must contain at least five characters
   • If you select a token as the authentication method, make sure you select an existing token
8. To set more granular account controls, open **Account Details**.
   **Regular User**
   • **Do not use device information for Full Disk Encryption remote help** - Enables user-bound remote help for the pre-boot user
   • **Lock user for preboot** - Locks the user for preboot
   • **Require change password after first logon** - Applies only to password authentication.
     Select this option to force users to change their password after the first pre-boot logon.
   **Note** - Regular User is the default option.

**Deployment User**
Deployment users are utilized when deploying Full Disk Encryption to client computers. When pre-boot log-on occurs with a deployment user, the user is forced to create a new pre-boot user and set a password. This new user is established as a regular user in the system.

Use the expire settings to make sure that the deployment user expires after the deployment is done. Remote Help for a deployment user is not possible after the expiration date has passed.

**Allow creating** option - limits the number of preboot accounts that can be created from this deployment user. The account expires after the maximum number of accounts is reached.

**Note** - the default option is for an unlimited number of preboot accounts.
9. To set an account expiration date, open the **Expiration Settings**.
   • **The user will expire after** - sets a number of preboot logons
     The default option allows an unlimited number of preboot logons.
   • **The user will be revoked after** - sets an expiration date. The default is: **Never**.

**Note** - Pre-boot users created from a deployment user have SSO and Password Synchronization capabilities. When the pre-boot user logs in for the first time, the pre-boot user is linked to the Windows user. The Windows account is used for SSO and Password Synchronization. Password Synchronization is active only if pre-boot authentication is enabled.
To unlink a Windows user from the logged on pre-boot account:
1. Open the Client UI Overview and click on the Full Disk Encryption Blade icon.
2. Click Unlink.
3. Enter the password of the logged on pre-boot account.
4. Click Unlink.
   A new link is created with a different windows account at the next Windows log in.

To add or remove a user from the Blocked Users List:
1. Open Smart Endpoint Manager.
2. On the Users and Computers tab, select an offline group.
3. In Group Details, click Edit.
   The Group Details window opens.
4. Click Pre-boot Users.
   The Pre-boot Users Details window opens.
5. In the Blocked Pre-boot Users area, click Add or Remove.

In-place Re-imaging

The in-place re-image feature lets you re-image partitions and maintain the Full Disk Encryption state.

Some of the required procedures are in the latest Dynamic Mount Utility Administration Guide

After the computer is re-imaged, install the same Endpoint Security client that was installed previously.

To prepare for in-place re-imaging:
1. Prepare a Windows partition image.
2. Prepare an environment that contains:
   • The Dynamic Mount Utility [see the Dynamic Mount Utility Administration Guide].
   • A folder with the prot_2k filter drivers [see the installation section of the Dynamic Mount Utility Administration Guide].
   • An application for re-imaging.

To use the image for in-place re-imaging:
1. Boot into the WinPE and unlock the drive with DMU.
2. Use the procedure in Using the Dynamic Mount Utility with a Boot disk to re-image the computer. Do NOT reboot after the re-imaging.
3. Install the prot_2k filter drivers on the system partition.
   In the command line, run: dism /image:C:\ /add-driver /driver:X:\drivers /forceunsigned
   Where X:\drivers is the location of the drivers in the example.
4. Reboot the computer.
5. Log in to Pre-boot to access Windows.
6. Deploy the Endpoint Security client with Full Disk Encryption on the re-imaged computer.
The computer is now running with the Endpoint Security client installed.

**AD Groups for Pre-boot Authentication**

In this release, you can add Active Directory users and groups to devices, OUs, or groups for Pre-boot authentication. In SmartEndpoint, groups have a new option of **Authorize Pre-boot nodes** in addition to **Authorize Pre-boot users**.

After you add a group to a device, group or OU, users in the group are directly assigned to the entity and do not need to go through user acquisition. If you add more users to the group after it was assigned to an entity, the new users are automatically directly assigned also.

The maximum amount of users in a group that can be assigned to a device, group, or OU for Pre-boot is 250.

**To add a group or user to a device and see authorized users:**

1. In the **Users and Computers** tab of SmartEndpoint, right-click a group or user. Select **User Authentication (OneCheck) > Authorize Pre-boot users**.
   The **Authorized Pre-boot users** window opens. From here you can:
   - See all users that are already assigned. The total number of users is shown in the bottom left corner.
   - **Add** and **Remove** users.
   - Search the results.
   - Click **Show all users** to toggle between showing all individual users in the group and showing included groups.

2. Click **Add** to add new users or group.
3. Select a device, OU, or group.
4. Click **OK**.

If a user does not have configured credentials, a **User Logon Pre-boot Settings** window opens. Configure credentials in the window and click **OK**. You can configure any supported authentication method for the user in this window.

You can add groups that contain users without configured credentials to a device, OU, or group, but the individual users without credentials are not assigned to the device. If credentials are configured for them, they will be assigned automatically based on the order in which they were added.

If you try to add an entity that will bring the total number of users over 250, the operation is blocked.
Managing Authorized Pre-boot Users and Nodes

- When users are added to an Active Directory group that has a Pre-boot assignment, the new users are automatically added as authorized Pre-boot users. If the new users bring the total Pre-boot users of a device above 250, a message shows that only the first 250 users are authorized to the device.

  A warning sign shows to the left of the group in the Authorized Pre-boot users window if one or more users in the group do not have credentials. Put your mouse over the warning sign to see a tooltip that explains the problem.

- A small warning sign on the corner of the group icon shows if all or some members of a group cannot be assigned to a device because the number of users is more than 250. Put your mouse over the warning sign to see a tooltip that explains the problem.

- When you click Show all users to show all individual users in the group, only users who are actually assigned to the device are shown. Users in a group that exceeded the 250 limit and were not added to the device are not shown.

- If you double-click a group in the Authorized Pre-boot users window, a new window opens with a list of all users in the group. Users that were not added to the device because the limit was reached are marked in red.

- Users are added to entities in this order:
  - Direct Users.
  - Inherited Users.
  - Direct Groups
  - Inherited groups

- You can see (but not edit) Authorized Pre-boot users and nodes from the Users and Computers tab > select a user or device > click User Authentication (OneCheck).

- You can see and edit Authorized Pre-boot users and nodes from the Users and Computers tab > Global Actions (on the left side of the window) > User Node Management.

- The Authorized Pre-boot Users tab shows who is assigned to an entity.
  - The Allowed On column shows the path where a user is assigned from or shows Direct if the user is directly assigned.

- The Authorized Pre-boot Nodes tab shows which entities a user is authorized to.
  - In the Authorized Pre-boot Nodes tab, the Allowed For column shows if the entity is allowed for the device directly or the path to a parent which is allowed on the device.
User-Bound Remote Help

User-bound Remote Help lets you do remote help for a user, Offline Group, or an organization without an exact device name. A special user is created for this purpose.

Note - User-bound Remote Help is less secure than regular Remote Help because the same key for Remote Help is distributed to all machines assigned to the specified user account.

To use user-bound Remote Help:

4. Click Next.
5. In the User and Authentication page:
   - Enter a Logon Name for a new user who will be used for user-bound Remote Help only, for example, Rhelp_User.
   - Enter and confirm a Password for the new user.
   - Select Do not use device information for Full Disk Encryption Remote Help.
   - Click Next.
6. In the Account details window:
   - Do NOT enter effective dates or an email address.
   - In the Account locations section:
     - Add nodes and users to allow Remote Help for them.
     - Remove nodes or users if Remote Help will not be allowed for them.
   
   Note - Entire Organization is included on the list by default. Make sure to remove it if necessary.
   - Click Next.
7. See the new Web Remote Help account in the list. Click OK. The new user shows under Other/Users Computers in the Users and Computers tab Directories tree.
8. Make the new user an Authorized Pre-boot User for a device, group, or OU:
   a) In the Users and Computers tab, right-click the object or node in the Directories tree.
   b) Select Full Disk Encryption > Authorize Pre-boot Users.
   c) Click Add to add the new Web Remote Help user.
   d) Click OK.
Notes -

- The password entered in the **User and Authentication** page of the **New Web Remote Help Account** wizard is for login to the Web Remote Help. An additional password is required to log in to Pre-boot on computers assigned to the user. This password can be the same or different as the Web Remote Help password. This behavior is different than a Web Remote Help account that is based on an Active Directory user, where only a Pre-boot password is required.

- When giving Full Disk Encryption user-bound Remote Help to a user through the Web Remote Help, this option shows in the Remote Help window: **Do not use device information.** If you select this, the Remote Help uses information from the user-bound Remote Help special user and does not use device information. The **Device Name** field is disabled.

### Offline Mode

Offline Mode lets users get policies and updates from a shared folder, without a connection to an Endpoint Security server. In this release, policies for these blades are supported in Offline Mode:

- Full Disk Encryption
- User Authentication (OneCheck)
- Common Client Settings

Manage the offline policies for these blades from each **Offline Group** in the Users and Computers tab. The policies for users in these groups are not configured in the Policy tab and are not included in policy installation.

**Workflow to Configure Offline Mode:**

- In the **Users and Computers** tab, create a new **Offline Group** and configure the sub-paths and settings.
- From the Offline Group, configure the policy for each blade.
- Export the required packages and put them in the configured sub-paths.
- Instruct users to install the packages from the sub-paths. Make sure they have the required access.

### Creating Offline Administrators

Offline administrators can be created one at a time or in groups.

**To create offline administrators:**

1. Open **SmartEndpoint Manager**.
2. On the **Users and Computers** tab, right-click an offline group.
3. Select **Create Administrators**.
   - The **Create offline group administrators** window opens with these options:
     - **Add Single User** - Adds one administrator
       - Enter the **Logon Name**.
Configure **Authentication credentials**, password or dynamic token.  

**Note** - you must select an existing token.

- **Add Users From File** - Imports offline administrators from a CVS file, and shows them in the table.
  Each imported administrator has a Logon Name, Authentication type and status.
  The Status column shows if an Administrator can be imported or not.
  A green V indicates if the offline administrator is ready for import.
  An X icon indicates offline administrators that cannot be imported. See the error message next to it.
  Click **Import** to import the administrators.

- **Remove User** - Removes an offline administrator. Select the administrator in the table.

## Configuring an Offline Group

Each Offline Group defines the location for its files and the included policies. Computers that install the package do not show in the tree on the **Users and Computers** tab.

For each group you configure a root path of the shared location where files for the group are stored, and sub-paths for each type of file. You must manually create each sub-path. Folders for these files are required. The default location is under the root path:

- **Updates** - Policy updates
- **Client Logs** - The location where logs from clients in this group are stored
- **Recovery Files** - Full Disk Encryption recovery files
- **Upgrades** - Upgrades to new client versions
- **Installation** - Complete installation packages

### To create an Offline Group:

1. In the **Users and Computers** tab navigation tree, right-click on **Offline Groups** and select **New Offline Group**.  
   The **New Offline Group** wizard opens

2. Enter this information:
   - **Offline group name** - A name for the group
   - **Root Path** - The root path of the shared location where files for this group are stored. This must be a valid UNC path or HTTP/HTTPS path. For example `\server\share\` or `http://server/share/`. HTTP/HTTPS paths are only supported when the WebDAV extension is enabled on the web server.
   - **Description** (optional) - Helpful information about the group or policies

3. Click **Sub-paths**.  
   The Sub-path Settings window opens

4. Select a **Category**. Each category has a default path under the defined root path. Keep the default or click **Add**, **Edit**, or **Remove** to change the path or add a new one.

5. Click **OK**.
6. Select a value for each of the Synchronization Settings:
   - Clients sync with shared location every X minutes
   - After a failed connection, clients retry to sync with shared locations every X minutes
   - Clients stop trying to sync with shared location after X failed attempts - This is only active when selected.

7. Click Next to configure the Policies for the group.

Configuring Policy for an Offline Group

The Group Details window in the Users and computers tab has changed for an existing offline group:

- The authorized pre-boot users list is now presented together with the blocked users list. This new dialog can be opened by clicking the Pre-boot Users button.
- The Pre-boot Users button has replaced the Blocked Users button. The Blocked Users dialog still shows in the Authorized Pre-boot Users wizard.

When creating a new offline group, the process remains the same.

Authorize Pre-boot Users

Continue with the New Offline Group wizard or click Authorize Pre-boot Users to configure the users who can log in to computers in the offline group.

- Click Add to add an authorized user
- Click Remove to remove a user
  Note - Removing a user from the Authorized Pre-boot user list will not remove the user from an already installed client. Use the Blocked Users feature to remove users on clients.
- Click Show all users to show the complete list
- Enter text in the Search field to search the list of users
- Click Blocked Users to create a list of users who are blocked from all computers in the offline group

Note - Smart Card authentication is not supported for Offline Pre-boot users. Select password or dynamic token as the authentication method.

Full Disk Encryption Policy

- Continue with the New Offline Group wizard or click Full Disk Encryption to configure the Full Disk Encryption policy settings for the group.

User Authentication (OneCheck) Policy

- Continue with the New Offline Group wizard or click User Authentication (OneCheck) to configure the User Authentication (OneCheck) policy settings for the group.
- This policy will be the default User Authentication (OneCheck) policy for acquired users and users created from the deployment users on the computer. The default policy can be updated with a policy Update.
If users are defined in SmartConsole, you can assign a different **User Authentication (OneCheck)** policy to them in SmartEndpoint. If users are acquired and not defined in SmartConsole, they always get the default policy.


**Common Client Settings Policy**

- Continue with the **New Offline Group** wizard or click **Common Client Settings** to configure the Common Client Settings policy settings for the group. All authorized users on a computer use the same **Common Client Settings** policy.


**Completing the Wizard**

- The Wizard shows the version and blades in the latest package.

- Click **Finish** at the end of the **New Offline Group** wizard. The Offline Group and all of its configurations and policies are saved. If you do not click **Finish** at the end of the Wizard, the group is not saved.

**Editing Pre-boot Users**

**To edit regular offline pre-boot user accounts:**

1. Open **Smart Endpoint Manager**.
2. On the **Users and Computers** tab, open **Offline Groups**.
3. Select the preboot user account
4. Select **Offline Pre-boot User Details** area and click **Edit**.

**To edit a deployment pre-boot account:**

1. Open **Smart Endpoint Manager**.
2. On the **Users and Computers** tab, open **Offline Groups**.
3. Select the preboot user account
4. Select **Deployment Pre-boot User Details** and click **Edit**.
Exporting Packages

Export the required packages and put them in the configured shared locations.

**To export packages:**

In the **Users and Computers** tab, right-click on the Offline Group and select an option:

- **Get Update Policy File** - Exports a file with policy updates.
  
  This file has CPPOL extension. The CPPOL file must be placed in the configured Updates folder.

- **Get Offline Management File (cpomf)** - Exports a CPOMF file that contains definitions that you can use to log in to the Endpoint Offline Management Tool.
  
  This is for a help desk or contractor environment that needs access to the Tool for Remote Help and creation of recovery media without access to an Endpoint Security server.

  To export all offline administrators:
  
  - Right click on an offline group and select **Get Offline Management File (cpomf)** or
  
  - Select multiple administrators in an Administrator OU under an offline group, right-click, and select **Get Offline Management File (cpomf)**.

- **Full Disk Encryption**
  
  - **Get Bypass Pre-boot File** - When installed, the computer bypasses Pre-boot based on the policy configured in the **Pre-boot Protection > Temporary Pre-boot Bypass settings** of the Offline group. The CPPOL file must be placed in the Updates folder.
  
  - **Get Revert Pre-boot to Policy Configuration File** - Returns the computer to the regular Pre-boot policy. The CPPOL file must be placed in the Updates folder.

- **Deployment**
  
  - **Get Initial Package** - Exports a complete MSI with the Offline Policy. This can be used for new client installation.
  
  - **Get Upgrade Package** - Exports a package to upgrade an existing offline client, and the updated CPPOL file. The details of the package are shown. Make sure the version is higher than the currently installed client version. You can select the **Export update offline policy** option to export a CPPOL file with the package.

    **Note** - Put the CPPOL file in the configured Updates folder and put the MSI in the configured Upgrades folder.

  - **Get Offline to Online File** - Exports a file that converts an offline client to an online client. After installation, the client will connect to the server that the file was exported from. See **Moving from Offline to Online Mode** for best practices.

    The CPPOL file must be placed in the Updates folder.

- **Advanced**
  
  - **Get Install Policy File** - Exports an installation policy file for the offline group. This is only necessary if you installed a client with an installation policy that contains shares that the client cannot access. The client remains in the installation state as the recovery file cannot be uploaded to the share.
Replace the installation policy located in the local Work folder on the client and reboot to continue the installation. The Work folder with the policy is located in:

On x64 client:
%PROGRAMFILES(X86)\CheckPoint\Endpoint Security\Endpoint Common\Work\n
On x86 client:
%PROGRAMFILES%\CheckPoint\Endpoint Security\Endpoint Common\Work\n
### Deploying Packages

**To deploy packages:**

Automatically deploy the offline client on computers or give users instructions to get the packages they require.

**To push a policy update for a specified client:**

Place the policy in the Work folder locally on the client, for example:
C:\Program Files\CheckPoint\Endpoint Security\Endpoint Common\Work.

If the client finds an update policy in the Work folder, the client makes sure that the update is new, imports it, and deletes the update from the Work folder.

The client then continues to use the normal update interval as configured.

**To update policies on specified clients:**

To update a specified computer, you can put an update policy in the client’s folder located in the Updates sub-path. When the client connects to the share it will check the Updates sub-path for new updates, but it will also check its own folder, located in the Clients folder. The client automatically creates this folder the first time it connects. The name of the folder is its hostname.

### Client Connections to Network Shares

Clients use the currently logged-in user to connect to the defined shares and search for update policies and to upload recovery files, logs, and status files. If there is no user logged-in or if multiple users are logged-in, the connection to the share is not available.

The logged-in user on the client must have these permissions on the share to be able to update and download files:

<table>
<thead>
<tr>
<th>Location</th>
<th>Read</th>
<th>Write</th>
<th>List</th>
<th>Execute</th>
<th>Modify</th>
<th>Delete</th>
<th>Create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Directory</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Recovery Files Directory</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Client Log Directory</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Moving from Offline to Online Mode

During the conversion from offline to online mode, all users acquired on the offline client are deleted. Users must be pre-authorized for the online client to make sure that there are authorized users on the client. If you move clients from offline mode to online mode, we recommend that you use these best practices:

- Configure at least one user that will be an authorized Pre-boot user on the client before and after the move to online mode. This will make sure there is an authorized Pre-boot user during the whole transition. This user can be removed after successful transition.
- If the logged-in authorized Pre-boot user is removed on the client during the move to online mode, a restart window opens. Wait for the automatic restart to occur.
- If no user has been authorized for Pre-boot for the online client, current offline users are not removed. These users remain with the OneCheck policy enforced in offline mode. When the first user for the online client is authorized for Pre-boot, the remaining offline users are removed. It can take up to 15 minutes before all offline users are removed.

Note - The move from offline to online Mode is permanent. It is not possible for an online client to move to offline Mode.

Endpoint Offline Management Tool

The Endpoint Offline Management Tool lets administrators manage offline mode users and give them password recovery and disk recovery. It does not require access to the Endpoint Security Management Server.

Double click the OfflineMgmtTool.msi file to install the tool.

Before you install the tool on a computer, make sure it has these prerequisites:

- We strongly recommend that the computer be protected by Firewall and Anti-Malware.
- Users must have administrator privileges.
- Microsoft Visual C++ 2017 must be installed.
- .NET Framework 4.5 must be installed.
Logging In to the Offline Tool

To log in to the tool, you must have a CPOMF file that contains at least one administrator with a password, or token authentication. To get the CPOMF file from SmartEndpoint, see: Get Offline Management File in Exporting Packages (on page 25).

1. Open the Offline Tool.
2. In the Login window:
   - CPOMF File - Browse to the location of the CPOMF file
   - Login Name - Enter an offline administrator name
   - Password/Token - According to the authentication method of the offline administrator, enter a password or token response.
     
     Note - If the authentication method is a token with a response length of 16 digits and you are authenticating with a response that is 8 digits long, you will be prompted to complete an additional challenge-response phase.
   - Click Login.

Password Recovery

To help a user log in to a locked computer click Password Recovery.

- Select Recovery Mode - Select the type of Full Disk Encryption Remote Help that is necessary:
  - One Time Logon - Lets users access using an assumed identity for one session, without resetting the password. Users who lose their Smart Cards must use this option.
  - Password Change - This option is applicable for users with fixed passwords who are locked out.

- Select Recovery File - The recovery file is a CPREC file that is uploaded from each client computer. The files are located in the Recovery Files shared folder.
  Click Browse to locate the file for the computer in the offline group that requires recovery.
  - Click Next.

Note - Each offline group is cryptographically independent. The CPOMF file for one group does not work for a different group.

Select a User

- Select a user that has Pre-boot permissions on the computer. You can enter the username manually in the format domain\username.
  - Click Next.

Challenge from User

- Response One - Tell the user to enter the Response One text string in the Remote Help window on the locked computer.
  The endpoint computer shows a challenge code.
- Challenge - Enter the challenge code that the user gives you.
**Response to User**

- **Response Two** - Tell the user to enter the **Response Two** text string in the Remote Help window on the locked computer.
  
  Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.

- **Try Again** - Click this to start the password recovery process again for a different user.

**Disk Recovery**

To help a user unencrypt a disk click **Disk Recovery**.

- **Select Recovery File** - The recovery file is a CPREC file that is uploaded from each client computer. The files are located in the Recovery Files shared folder.
  
  Click **Browse** to locate the file for the computer in the offline group that requires recovery.

  - Click **Next**.

  **Note** - Each offline group is cryptographically independent. The recovery file for one group does not work for a different group.

**Select a User Account**

- Click **Add** to manually enter a new temporary user that will log in with the recovery media.

  - Click **Next**.

**Select Media**

- Select the type of recovery media to generate:
  
  - **ISO file**
  - **REC file**
  - **USB media**

  If you select ISO or REC, select the storage location.

  If you select USB, choose the drive to use.

  - Click **Create Media**.

  **Note** - To create USB media, the tool must run with administrator privileges and the Media Encryption & Port Protection must be disabled.
External PKI Certificates

By default, Check Point servers and clients use certificates signed by the internal Check Point Certificate Authority (CA) for client-server communication, authentication, and data encryption. In this release you can overwrite the default certificates with certificates generated by an external CA.

These types of certificates are supported in .p12, .pem, and .crt formats:

- **CA** - Public certificate that is used to validate other certificates issued by the same CA. It is installed on clients using Push Operations.
- **SSL** - Certificate for the Apache server component of each server for SSL communication.
- **Remote Help** - The Full Disk Encryption blade installed on the client uses this certificate to work with the Remote Help server for password recovery.
- **Unlock on LAN** - The Full Disk Encryption blade installed on the client uses this certificate for authentication with the Unlock on LAN feature.

Import certificates and install them on servers and clients, as necessary.

Importing Certificates

The import procedure is the same for all types of external certificates.

SSL certificates must contain a server DN. If they contain a DN for a server which does not exist, a warning shows. The user can choose to proceed.

**To import an external certificate:**

1. Open SmartEndpoint.
2. Go to Manage > Certificate Management.
3. Click Import.
   The Import Certificate Wizard opens.
4. On the Import Certificate page:
   a) Insert the certificate file. You can drag and drop the file into the window or navigate to it from the folder icon.
   b) Select the certificate type.
   c) [Optional] Enter the file’s password.
   d) [Optional] Enter a descriptive comment.
5. Click Next.
   See Certificate Imported Successfully.
6. If the imported certificate requires a private key and does not include it, the Import Private Key page in the Import Certificate wizard will open:
   a) Insert the private key file. You can drag and drop the file into the window or navigate to it from the folder icon.
   b) Enter the file’s password, if necessary.
c) Click Next.
d) Click Finish.

7. If the imported certificate does not include a CA certificate, the Import CA page in the Import Certificate wizard will open:
   a) Insert the file. You can drag and drop the file into the window or navigate to it from the folder icon.
   b) Enter the file’s password, if necessary.
   c) Click Next.
       See Private Key Imported Successfully.
   d) Click Finish.

8. Click Finish.

Installing CA Certificates on Clients

To install a CA certificate:
1. Open SmartEndpoint.
2. In the Users and Computers tab, under Global Actions, select Push Operation.
   The Create Push Operation wizard opens.
4. Select the computers to push the certificate to.
5. Click Next.
6. Click Manage.
7. Select the certificate and click Assign.
8. [Optional] Enter a descriptive Comment.
9. Click Next.
10. Click Finish.

A SmartEndpoint notification shows the number of clients the certificate was pushed to.
See the Push Operations report in the Reporting tab for more information about the operation.

Installing SSL Certificates on Servers

To install an SSL certificate on an Endpoint Security server:
1. Open SmartEndpoint.
2. Go to Manage > Endpoint Servers.
3. Select a server and click Edit.
   The Endpoint Server Wizard opens.
4. Click Next.
5. Click Manage to select an SSL certificate for the server.
6. Select the relevant certificate from the list and click Assign.
   Note - The server name in the Issued To field of the selected SSL certificate should be identical to the server’s DN. Hover over the selected certificate to see the complete information.
7. Click Next.
8. Select the server with the new certificate to Install Database.
9. Click Finish.
   See the installation process finish.
10. In a High Availability environment, Install Database again on the secondary server.

Replacing SSL Certificates in an Existing Environment

We recommend that you implement the new SSL certificates gradually. After an SSL certificate is replaced on a server, clients who do not have the related CA certificate will not be able to send SSL messages (for example, Full Disk Encryption blade payloads and Audit logs) to that server.

To replace SSL Certificates in an existing environment:
1. Import a new CA certificate.
2. Import a new SSL certificate for each server.
3. Use Push Operations to push the new CA certificate to a small OU or group of devices.
   A device will report the push operation at 20% with this message: CA certificate received by Endpoint. This occurs when it has downloaded new CA certificate and is trying to find a server with an SSL certificate signed by same CA.
4. Install the new SSL certificate on one of the servers accepting clients.
5. Wait for all of the clients’ Push Operation status to be completed.
6. Repeat step 2 to gradually migrate more servers to new SSL certificates.
   Repeat steps 3-5 to migrate more clients.
   Do the procedures on the primary and secondary servers last.

Installing Full Disk Encryption Certificates

To install a Remote Help or an Unlock on LAN certificate:
1. Open SmartEndpoint.
2. In the Users and Computers tab, select the Entire Organization folder, and click Manage Certificates.
3. Click the Manage button next to Remote Help Certificate or Unlock on LAN Certificate.
4. Select the Remote Help or Unlock on LAN certificate and click Assign.
5. A message shows, asking if you would like to install the policy now. Click Yes or No.
6. If you clicked Yes to install the policy, a message shows that all changed data must be saved. Click Yes to save changes and continue.
7. Click Install.

Installing Certificates for Offline Groups

Offline Groups can use external certificates for Remote Help. The default setting is Use internally generated certificate, which uses the internally generated certificate.

To install an external certificate for an Offline Group:
When creating an offline group:
   a) In the Offline Group Settings, select Select existing certificate.
b) Click Manage and select the certificate from the list or click Import to get the certificate.

c) Click Assign.

d) Continue with the New Offline Group wizard, as described in Configuring an Offline Group (on page 22).

When editing an existing offline group:

a) Go to Group Details and click Edit.

b) Click Manage and select the specific certificate.

c) Click OK.

Troubleshooting

You can monitor the certificates on each server and computer from the Reporting tab > Activity Reports > Endpoint Connectivity.

These columns of the report relate to the certificates installed (the columns are hidden by default):

- **Active Certificate** - Shows the details of the currently active CA certificate on the computer.

- **StandBy Certificate** - Shows the details of a CA certificate in standby state on the computer. This CA is not used but can be used in the future.

- **Active Certificate Applied On** - Shows the date when the currently active CA certificate became active.

SHA-256 Certificate Support

For clean installations, the management certificate can be encrypted with SHA-256 encryption. In existing environments, SHA-256 is not supported for the Root CA. You can use SHA-256 for renewed certificates after the previous certificate expires.

**To activate a certificate with SHA-256 on a new R77.20 installation:**

1. Install a new R77.20 Endpoint Security Management Server.
   This command changes the certificate hash to SHA-256 from SHA-1, which is the default.
3. Run: `fwm sic_reset`
   This command resets the internal CA.

   **Important** - Do NOT run this command on a server that has Endpoint Security clients deployed. The clients will lose all connectivity to all servers.

4. Run: `cpconfig` and select Certificate Authority > Initialize.
   The new Internal CA certificate is created and signed with SHA-256.
5. Run: `cpstart`
6. Install this release.
7. Connect to the Endpoint Security Management Server with SmartDashboard and enable the Endpoint Policy Management blade.
To configure a renewed certificate to use SHA-256:
On the Endpoint Security Management Server, run:
```
cpca_client set_sign_hash sha256
```
After the management certificate expires, the renewed certificate will be signed with SHA-256 encryption.

### TLSv1.2 Support

By default, the Endpoint Security servers in this release support TLSv1.2 and TLSv1 for communication between clients and servers.

**To configure servers to support TLSv1.2 only:**

1. On each Endpoint Security server, open `$UEPMDIR/apache22/conf/ssl.conf`.
2. Run: `cpstop`
3. Change the attribute `SSLProtocol +TLSv1 +TLSv1.2` to: `SSLProtocol TLSv1.2`
4. Save changes.
5. Run: `cpstart`

### Local Deployment Options

When you use Automatic Software Deployment, you can configure clients to use local storage to upgrade Endpoint Security clients. This lets administrators use Automatic Software Deployment, without the need for each Endpoint Security client to download a package from the Endpoint Security Management Server.

To set up such a deployment, you must:

- Upload the packages to the Endpoint Security Management Server.
- Create a Software Deployment rule with the package version selected.
- Configure a Client Settings rule to allow deployment from local paths.
- Upload the packages to the defined local storage paths

This is only supported on Windows clients.

**Note:** If local deployment is enabled for a client, the administrator can still choose whether clients try to download packages from the Endpoint Security Management Server if packages are not found in local storage. This option is called: **Enable Deployment from server when no MSI was found in local paths**.

**To enable Software Deployment with a locally stored package:**

2. Put the same packages in local storage location on client computers, for example `C:\TEMP\EPS\32bit\EPS.msi`.
3. Go to the **Policy** tab of SmartEndpoint > **Client Settings** rule.
4. In the Deployment Locations action, select **Enable deployments from local paths**. You can also **Clone the action**.
5. Double-click the action.
The Deployment Locations window opens.

6. Make sure that **Allow to install software deployment packages from local folders** is selected.

7. Optional: Select **Enable Deployment from Server when no MSI was found in local paths**. When selected, if no MSI file is in the local paths, the client checks the Endpoint Security Management Server for packages.

8. Click **Add item** and select the **Package Location** to add paths for packages located on client computers. Select if each package is for 32 bit or 64 bit computers.

9. Click **OK**.

10. In the Deployment tab, create or edit a Software Deployment rule to use the package **Version** and assign it to computers.

11. Click **Save**.

12. Install Policy to deploy the rule to clients.

**Note** - If the version of the Endpoint Security client in the Software Deployment rule and in the local file path is not the same, the client is not deployed.

If the version on the server and in the local file path are not the same, an error shows.

---

### Reporting Features

#### Changes in Reporting

From the **Reporting** tab > **Options** icon > **Export Report**, reports are now faster and can only be exported to MS Excel. It is not required to have Excel installed on the computer.

Within reports, you can filter in each column. When you filter the report results, the information in the graphical section of the page changes to reflect the filtered results.

#### Policy Reports

A policy report shows information about the assigned policies on each Endpoint Security Client computer in the organization. You cannot see the Policy Report in SmartEndpoint. It is a CSV file that is created on the Endpoint Security Management Server at scheduled times.

**To enable scheduled Policy Reports:**

1. On the Endpoint Security Management Server, run: `cpstop`

2. Open the server's **local.properties** file:
   
   `$UEPMDIR/engine/conf/local.properties`

3. Find the line: `#emon.scheduler.time=9:55:00,10:55:00,15:33:00`
   
   - Delete the `#` from the line
   - Edit the times to show the hour when the reports will be created. Reports will be created each day at these times.
   - Make sure the line is in this format:

     ```sql
     emon.scheduler.time=HH:mm:ss,HH:mm:ss,HH:mm:ss
     ```

     with no spaces between the times and commas.
4. Find the line: `#emon.scheduler.max.reports=10`
   - Delete the `#` from the line
   - The number represents the maximum number of reports that can remain in the report directory. The oldest ones are overridden by newer ones. Optional: Edit the number.
   - Make sure the line is in this format: `emon.scheduler.max.reports=<number of reports to save>`.

5. Find the line: `#emon.scheduler.policyreport=true`
   - Delete the `#` from the line
   - Make sure the line is in this format: `emon.scheduler.policyreport=true`

6. Create a new folder: `$FWDIR/conf/SMC_Files/uepm/reports`
   Run: `mkdir $FWDIR/conf/SMC_Files/uepm/reports` `chmod 2777 $FWDIR/conf/SMC_Files/uepm/reports`
   The name of the report will be: `policyReport<number>.csv`
   The number represents the creation time so newer reports have higher numbers.

7. Run: `cpstart`

When a Policy Report is generated, it includes these fields:

- **General fields**:
  - User Name - `ntlocal` for local user, `ntdomain://<DOMAIN-NAME>/<USER LOGON NAME>` for domain users
  - Computer Name - Name of the computer
  - User Location - User domain distinguished name (empty for local users)
  - Group Names - The names of the groups the user is in
  - IP Address - The most updated IP address of the device
  - Last Contact - The last time the computer had contact with the Endpoint Security Management Server
  - OS Name - The full name of the Operating System, for example: `Windows 8.1 Professional Edition`
  - OS Version - The version of the Operating System, for example: `6.2-9200-SP0.0-SMP`
  - OS Type - Workstation or Server
  - Machine Type - Laptop or Desktop
  - Domain Name - Active Directory domain, if relevant

- **Policy** (includes User Authentication (OneCheck), Full Disk Encryption, Media Encryption & Port Protection, and Common Client Settings):
  - `<Blade> ID` - A unique identifier of a policy rule that applies to the user or computer
  - `<Blade> Name` - The rule name (given by the administrator)
  - `<Blade> Description` - The rule comment (given by the administrator)
  - `<Blade> Actions` - The names of the rule actions
  - `<Blade> Version` - The version of the rule
  - `<Blade> Modified By` - The name of the administrator that last modified the rule
  - `<Blade> Install Time` - When the blade was installed on the client
  - `<Blade> Inherited From` - The Active Directory path the rule was originally assigned on and inherited by this machine.
Certificate Expiration Alerts

Certificate Expiration alerts show if certificates are going to expire soon. On the Alerts page of the Reporting tab, configure when alerts are triggered and when email notifications are sent. When the alert is triggered, a message shows in the Active Alerts section of the SmartEndpoint Overview.

Note that Trend and Endpoint graphs are not relevant for this alert.

To configure settings for Certificate Expiration alerts:
2. In the Alerting Threshold Settings section, select how many days before a certificate expires alerts are triggered.
3. In the Notification Settings area:
   - Notify on alert activation - Select to send an email notification when an alert is activated.
   - Notify on alert resolution - Select to send an email notification when a certificate that had triggered an alert is renewed.
   - Remind every - Select the frequency of the alert activation reminder emails.
   - Click Add to enter email addresses to receive the notifications.
4. Click OK.
5. Install Policy.

AD Users and Groups for SmartConsole Authentication

This release supports Active Directory user authentication for SmartConsole applications.

The workflow to configure Active Directory users and groups for SmartConsole authentication includes:
- Create a new Active Directory account in SmartDashboard.
- Configure Active Directory group or user administrator permissions.

To create a new Active Directory account:
1. In SmartDashboard, right-click Check Point and select Check Point > Security Gateway/Management.
2. In the window that opens, click Classic Mode. A new gateway Properties window opens.
3. Enter a Name and the IP Address for the new Machine.
4. Select Identity Awareness.
   - Identity Awareness Configuration wizard starts.
5. Select Browser-Based Authentication and click Next.
6. Select **Create new domain** and fill in these:
   - **Domain Name**
   - **Username**
   - **Password**
   - **Domain Controller** IP address

7. Click **Connect**.
   If connection to the Domain Controller is successful, this message shows: **Successfully connected!**

8. Click **Next**.

9. Click **Next**.

10. Click **Finish**.

11. Click **Cancel**.
    The Active Directory account is created, but the gateway object creation is not necessary.

To configure **Active Directory group or user administrator permissions**:

1. In SmartDashboard, select **Users and Administrators**.

2. Right-click **Administrators** and select **New LDAP Administrator/Group**.
   The Administrator Properties window opens.

3. Enter a **User Name**. This can be any name and is only for display.

4. Click the button next to **Login DN**.

5. Select an AD entity.
   The window shows the Active Directory information for the entity.

6. Click **OK**.
   The entity's AD distinguished name is shown in the **Login DN** field.

7. Click **OK**.

8. Click **Save**.

To **log in with Active Directory credentials**:

1. Open a SmartConsole application.
   The login window opens.

2. Enter your AD credentials and select the AD from the list.

---

**Strengthening the LDAP Communication**

By default Active Directory authentication is done with the LDAP protocol and simple authentication method. You can change this to LDAPS with or without GSSAPI (Kerberos v5) authentication.

**To change the authentication protocol to LDAPS, GSSAPI, or both:**

1. Open the `$UEPMDIR/engine/conf/ldap.utils.properties` file.

2. Configure the protocol or protocols to use.
   - **To configure LDAPS** - Change `use.ssl=false` to `use.ssl=true`
   - **To configure GSSAPI** - Change `use.gssapi=false` to `use.gssapi=true`

Both LDAPS and GSSAPI can be set to true.
3. Save.

For GSSAPI, no additional configuration is necessary.

**Additional steps for LDAPS:**

- Configure the Domain Controller to use LDAPS.
- Import all Domain Controller certificates to the Endpoint Security Management Server keystores.

**To import a certificate to the Endpoint Security Management Servers (Primary and Secondary in High Availability):**

1. Find the index of the SSL certificate: On a domain controller which is configured to support LDAPS, run: `certutil -store -v MY`

   The output of this command is a list of certificates. The certificates are separated by a line like this:
   
   `================ Certificate 0 ================`
   
   where 0 is the index number of the certificate.

2. Find a certificate that has:
   - Subject: DC FQDN
   - One of certificate extensions is **Server Authentication OID 1.3.6.1.5.5.7.3.1**.

3. Get that certificate’s index number this is number which appears in separation header before each certificate (in this example it is 0).
AD Users and Groups for SmartConsole Authentication

X.509 Certificate:
Version: 3
Serial Number: 610206fb000000000002
Signature Algorithm:
  Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
  Algorithm Parameters:
    05 00
Issuer:
  CN=mulberry-DC-CA
  DC=mulberry
  DC=com

NotBefore: 23/06/2014 13:12
NotAfter: 23/06/2015 13:12

Subject:
  CN=DC.mulberry.com

Public Key Algorithm:
...

Certificate Extensions: 9
  1.3.6.1.4.1.311.20.2: Flags = 0, Length = 22
  Certificate Template Name (Certificate Type)
    DomainController

  2.5.29.37: Flags = 0, Length = 16
  Enhanced Key Usage
    Client Authentication (1.3.6.1.5.5.7.3.2)
    Server Authentication (1.3.6.1.5.5.7.3.1)
...

4. To download a certificate from the domain controller, run:
certutil -store MY <certificate index> <file name>
For example: certutil -store MY 0 C:\certificates\DCCert.cer

5. To import a certificate to Endpoint Security servers, copy the file to the Endpoint Security servers (primary and secondary) and run:
cd $UEPMDIR/engine/jre
./bin/keytool -import -keystore ./lib/security/cacert -file <cert file name> -alias <alias>
For example: ./bin/keytool -import -keystore ./lib/security/cacert -file /certif/DCCert.cer -alias DCSSLCert

Known Limitations

These limitations apply to this release:

Active Directory

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01382828</td>
<td>Adding Active Directory users with the same login names as Internal users is not supported.</td>
</tr>
</tbody>
</table>

Full Disk Encryption

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| 01431925 | 1) When you add credentials to a user that is being assigned in the Authorized Pre-boot users window, the credentials are not saved on the server until you press OK in the Authorized Pre-boot users window.  
2) When you add credentials to a user through More info in Users and Computers, the credentials are not saved on the server until you click the save icon.  
For these reasons, newly added groups and existing groups in the Authorized Pre-boot users window can be shown as groups in which some users have no credentials. User might have acquired credentials that are not yet saved on the server. |
| 00674336 | If you configure the setting “Show Pre-boot logon screen” to 0 minutes for Temporary Pre-boot bypass, issues might occur. To prevent issues, do not set the value below the default value (1 minute). |

Offline Mode

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To give Remote Help or create recovery media for offline clients, you must use the Endpoint Offline Management Tool.</td>
</tr>
<tr>
<td></td>
<td>There is no support for Smart Card user acquisition.</td>
</tr>
<tr>
<td></td>
<td>The Unlock on LAN feature is not supported.</td>
</tr>
<tr>
<td></td>
<td>If user acquisition is enabled and a number of acquired of user are required to enable Pre-boot, then acquisition of all users must be made before a reboot occur to complete the installation. A reboot will remove all previously acquired users if the installation is not finished.</td>
</tr>
</tbody>
</table>
## General

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01380031</td>
<td>Simultaneously exporting several packages is not supported.</td>
</tr>
<tr>
<td></td>
<td>Only Full Disk Encryption and Media Encryption blades are supported.</td>
</tr>
</tbody>
</table>

## Management

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A SmartDashboard administrator cannot log in to the Web Remote Help portal.</td>
</tr>
<tr>
<td></td>
<td>SmartDashboard and SmartEndpoint cannot connect to the Secondary server if the initial load is not completed.</td>
</tr>
<tr>
<td>01625569</td>
<td>After installation of this release, Apache configuration files are upgraded and all customization is removed. Previous configuration files are backed up in the $UEPMDIR/apache22/conf folder.</td>
</tr>
<tr>
<td>01646143</td>
<td>The Self Help portal can be enabled on other servers but only works on the primary server.</td>
</tr>
<tr>
<td>01281459</td>
<td>The password for Client Uninstall must be in English.</td>
</tr>
</tbody>
</table>

## Media Encryption & Port Protection

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01619782</td>
<td>No remote help support for encrypted CD/DVD.</td>
</tr>
<tr>
<td></td>
<td>Endpoint R73 ME cannot work in parallel to E80 offline FDE.</td>
</tr>
</tbody>
</table>

## Certificates

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01970658</td>
<td>When replacing an SSL certificate on a server, the Apache server needs to restart in order to reload the new certificate. In some cases the restart action times-out and Apache stays down. If this occurs: launch the Apache server manually either from Services.msc or using the cpstart command.</td>
</tr>
<tr>
<td>00674967</td>
<td>Mac clients do not support external PKI certificates.</td>
</tr>
</tbody>
</table>