26 July 2015

Check Point Endpoint Security

R77.20 - EP 5.6

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.

**Additional Information**

Visit the Check Point Support Center [http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 July 2015</td>
<td>General updates</td>
</tr>
<tr>
<td>16 July 2015</td>
<td>Added operating systems in System Requirements (on page 7).</td>
</tr>
<tr>
<td>13 July 2015</td>
<td>Added this table for revision changes.</td>
</tr>
<tr>
<td>9 June 2015</td>
<td>Replaced incorrect “Linux only” (“Installation” on page 8) with Gaia only on the server.</td>
</tr>
<tr>
<td>4 June 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

**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 R77.20 - EP 5.6 Release Notes].
Introduction

Thank you for installing Check Point Endpoint Security R77.20 - EP5.6 with Hotfix. This is a special release for new Endpoint Security clients, and can be installed on a machine running E75.20 VPN client.

This release includes an Endpoint Security Client for Windows and a new SmartConsole.

What's New

This release for Endpoint Security includes these new features:

Server Side
- Full Disk Encryption Self-Help Portal
- SHA-256 Certificate Support
- Support for TLSv1.2 communication between client and servers
- Changes in Reporting
- User-bound Remote Help
- Policy caching for increased security
- Support for Active Directory users and groups for authentication to SmartConsole applications
- Migration of R73 Media Encryption Remote Help keys
- New Policy Report
- The SmartConsole fingerprint uses SHA-2 encryption.
- General Performance improvements

Client Side
- Self-Help for Full Disk Encryption
- Full Disk Encryption Offline Tool
- Patch Management
- Temporary Pre-boot Bypass with connection to LAN
- In-place Re-imaging
- Offline Mode
- Support for client package deployment from shared file paths and URLs
- Support for Active Directory group assignment for Pre-boot authentication
System Requirements

The client can be installed on these operating systems:

- **Windows 8.1** 32/64-bit, with or without Update 1 [Editions: Pro and Enterprise editions]
- **Windows 8** 32/64-bit [Editions: Professional and Enterprise editions]
- **Windows 7** 32/64-bit with or without SP1 [Editions: Ultimate, Professional and Enterprise editions]
- **Windows Vista** 32/64-bit [SP1 and above Enterprise & Business edition]
- **Windows XP** 32-bit Professional [SP3]

When deploying Full Disk Encryption on Windows 8 and higher in UEFI mode, Windows 8 logo certified hardware with UEFI version 2.3.1 or higher is required.

R77.20 - EP5.6 with Hotfix clients work with R77, R77.10, and R77.20 Endpoint Security servers.

For system requirements, see the *R77.20 Release Notes*

Supported Upgrade Paths on Clients

Only Media Encryption and Full Disk Encryption clients are supported in this version.

The client can upgrade from these versions:

<table>
<thead>
<tr>
<th>Package Type</th>
<th>Windows 7</th>
<th>Windows 8.1 / Windows 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Full Disk Encryption</td>
<td>7.4.5, 7.4.8, 7.5.1 HF2, HF10</td>
<td>7.5.1 HF2, HF10</td>
</tr>
<tr>
<td>Online Full Disk Encryption and Media Encryption</td>
<td>E80.32 and above</td>
<td>E80.42, E80.51</td>
</tr>
</tbody>
</table>

Supported Upgrade Paths on Servers

Endpoint Security Management Server, connection points, and High Availability server can run only on Gaia. You can upgrade the server from these releases to R77.20:

<table>
<thead>
<tr>
<th>Version On Gaia</th>
<th>Upgrade Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>R77, R77.10</td>
<td>Install the appropriate upgrade package. See Gaia Installation and Upgrade Packages.</td>
</tr>
<tr>
<td>R76</td>
<td></td>
</tr>
<tr>
<td>R75.40, R75.45, R75.46, R75.47, R75.40VS</td>
<td>To upgrade to Gaia, install the appropriate upgrade package. To upgrade to other platforms: upgrade first to R77</td>
</tr>
<tr>
<td>R75, R75.10, R75.20, R75.30</td>
<td>Upgrade first to R77.</td>
</tr>
</tbody>
</table>
### Offline 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></td>
</tr>
<tr>
<td></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++ 2008 SP1 Redistributable Package
- .NET framework 4.5
- OS: Windows 7, 8, 8.1 - 32- and 64-bit

### Installation

This release includes 2 hotfixes that must be installed on a Check Point R77.20 Management Server. If you have multiple Endpoint Security servers in an environment, install the hotfixes on all servers.

#### To install the hotfixes on an Endpoint Security server:

1. Install the fw1_wrapper hotfix:
   - a) Copy `fw1_wrapper_HOTFIX_R77_20_EP05_GA_FIX1_002.tgz` from the `fw1_wrapper_hotfix` folder to `/var/tmp`.
   - b) Unzip the tgz.
   - c) Run the unzipped executable.

2. Install the uepm hotfix:
   - a) Copy `uepm_HOTFIX_R77_20_EP05_GA_FIX1_002.tgz` from the `uepm_hotfix` folder to `/var/tmp`.
   - b) Unzip the tgz.
   - c) Run the unzipped executable.
Upgrading with Online Synchronization

To upgrade to this release in an environment that uses online synchronization:

1. On each Endpoint Security Management Server, and Remote Help Server, run:
   /opt/CPshrd-R77/bin/PgOnlineSyncUtil stop_engine
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.
7. 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) Wait until the sync is completed.
   b) Run: PgOnlineSyncUtil is_initial_load_over on the secondary and Remote Help Servers and make sure they are finished.
   c) Check the Management High Availability state in SmartDashboard. Make sure that the state is Synchronized with no error.

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.

To enable the Self-Help Portal:

On the Endpoint Security Management Server, run:

```
cd $UEPMDIR/engine/jre/bin/
sselfhelp_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:

```
sselfhelp_cmd disable
```

To query the status the Self-Help Portal, run:

```
sselfhelp_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 Recovery action and select Edit.
2. Select Allow password Self-Recovery 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 password Recovery.
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 password 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 Enrollment to force the user to re-register to the portal.
   Select Lock Password Recovery 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 12)
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 start 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.
Creating Pre-boot Users

To create new Pre-boot users:
1. Go to Authorized Pre-boot Users.
2. Click New.
   A dialog window opens to add a new Pre-boot user.
3. Enter the login name and password.
   Note - The password must be at least 5 characters in length.
4. To set the user as an RH bound user, click the Do not use device information for Full Disk Encryption remote help box.
5. To lock the user for Pre-boot, click the Lock user for Pre-boot box.

Another method to create a new Pre-boot user:

In Users and Computers, right-click Other Users\Computers > Full Disk Encryption > Add new preboot user. The same dialog window opens. Unlike the first method, the created user is not assigned to any node.

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.
2. On the Endpoint Security Management Server, run: cpcaclient set_sign_hash sha256
   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: cpcaclient set_sign_hash sha256

After the management certificate expires, the renewed certificate will be signed with SHA-256 encryption.
In-place Re-imaging

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


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.

TLSv1.2 Support

This release supports TLSv1.2 communication between client and servers. By default, Endpoint Security management only supports TLSv1.

To configure support for different TLS versions:

2. Change the attribute SSLProtocol TLSv1 in one of these ways:
   - To support only TLSv1.2, change it to: SSLProtocol TLSv1.2
   - See the Apache 2.2 documentation.

   Note: Endpoint Security client before this version can only work with TLSv1.
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.

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.

To support all TLS versions but not SSL, change it to: `SSLProtocol All -SSLv2 -SSLv3`

3. Save changes.
4. Run: `cpstop`
5. Run: `cpstart`
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

**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
- 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.

**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 all acquired user 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.

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.

- 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. It 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.

  When you create the file, you define a login name and password that administrators can use to log in to the Endpoint Security Offline Management Tool.

- 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.

  - Get Revert Pre-boot to Policy Configuration File - Returns the computer to the regular Pre-boot policy.

- 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 show. Make sure the version is higher than
the currently installed client version. An option shows to Export update offline policy. If you select this, a policy update exports with the package.

**Note** - Put the policy in the Updates folder and put the MSI in the 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 (on page 19) for best practices.

- **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 reach. The client will then get stuck 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.

### 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. Do not click OK. 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++ 2008 SP1 Redistributable Package must be installed.
- .NET framework 4.5 must be installed.
Logging In

To log in to the tool, you must have a CPOMF file, login name, and password that you configure in SmartEndpoint.

To get the CPOMF file, login name, and password from SmartEndpoint:

1. Right-click on the Offline Group folder in SmartEndpoint and select Get Offline Management File.
2. Select a location for the CPOMF file.
3. Define a Login name and password that will be necessary to log in to the Endpoint Offline Management Tool.

In the Login window:

- **CPOMF File** - Browse to the location of the CPOMF file.
- **Login Name** - Enter the login name that you defined when you generated the Get Offline Management File.
- **Password** - Enter the password that you defined when you generated the Get Offline Management File.
- 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** - One Time Login 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.
Patch Management

Patch Management is a way to install small Endpoint Security client fixes on computers without a whole upgrade package. Configure the policy related to patches in SmartEndpoint.

When a patch is installed on a client computer, end-users see the same windows and messages as with regular Software Deployment. After the patch installation, client computers must restart.

About Endpoint Security patches:
- Patches are for Windows computers only with different files for 32 and 64 bit.
- Patches are cumulative - each one includes the earlier patches for the same version.
- The extension of the patch files is .MSP (not MSI).
- An example of the naming convention for patches is: EPS.8.4.294.1234.1.64.msp
  Explanation: EPS.<build number of the client (8.4.294)>.<4 digit patch number (1234)>.<1 digit that show the type of patch (1)>.<64 or 32 which shows the bits of the system that it is for>.

Configuring Patch Management

To enable clients to install patches in online mode:
1. Go to the Policy tab of SmartEndpoint > Client Settings rule.
2. In the Deployment Locations action, select Enable deployments from local paths. You can also Clone the action.
3. Double-click the action.
   The Deployment Locations window opens.
4. Make sure that Allow to install software deployment packages from is selected.
5. Click Add item and select Patch Package Location. You can add multiple paths.
   The client searches from all defined paths for the highest available patch for the installed Endpoint Security version.
6. Click OK.
7. Click Save.
8. Install Policy to deploy the rule to clients.
9. Put the Patch files, for example: EPS.8.4.294.1234.1.64.msp, in one of local storage location paths that you defined as a Patch Package Location.

To enable clients to install patches in offline mode:
1. Select an offline group
2. Select Client Settings and click Edit rule.
3. In the Deployment Locations action, select Enable deployments from local paths.
4. Right-click the action and select Edit Shared Action or Clone the action.
5. Make sure that Allow to install software deployment packages from is selected.
6. Click Add item and select Patch Package Location. You can add multiple paths.
   The client searches from all defined paths for the highest available patch for the installed Endpoint Security version.
7. Click **OK**.
8. Click **OK**
9. Click **Next** and **Finish**.
10. Right-click on the offline group, and select **Get Policy Update File**.
11. Save the update file `cp_offline_update.cppol`
12. Copy the file to the Update subfolder in the Offline Location: `<ROOT PATH>\Updates`
13. Put the patch files, for example: `EPS.8.4.294.1234.1.64.msp`, in one of local storage location paths that you defined as a **Patch Package Location**.
   
   Endpoint Security client computers in the group will get a patch management request and an update will start.

**Note** - Do not change patch file names.

**Installing patches manually on client computers**

You can install patches manually. It requires a Client Uninstall Password. If you do not have a Client Uninstall Password configured, create one in **Policy** tab> **Common Client Settings** rule > **Installation and Upgrade Settings** action.

1. Copy the patch to the computer.
2. Open the command prompt as an administrator.
3. Enter the complete patch file name in command prompt, for example, `EPS.8.4.294.1234.1.64.msp` and press Enter.
   
   A window opens asking for the Client uninstall password.
4. Enter the password to start the patch installation.
5. Restart the computer when prompted.

**Patch Information on Client Computers**

To see installed patches in the Control Panel:

Go to **Control Panel** > **Programs** > **Programs and Features** > **View installed updates**.

To see the highest installed patch in the Client UI:

- See the Client Overview > **General Info > Version**.
- Right-click the client icon and select **About**.

To see installed patches in the Registry:

- In Check Point > Endpoint Security:
  - **VersionPatch** - Version of the highest installed patch.

In Check Point > Endpoint Security > Device Agent > Patch Status. For each installed patch there is a key, with a patch name inside each key, for example: `8.4.295.1234.1.64`.

- **PatchVer** - Patch version number.
- **TargetEps** - Version of the Endpoint client the patch is for.
- **State** - State of the patch, for example Installed, Scheduled or Installing.
• In Check Point > Endpoint Security > Device Agent > Deployment Status:
  • HighestPatchVersion - A new entry that shows the highest installed patch.

Patch Information on Endpoint Management

Patches installed on Endpoint Security clients are shown in SmartEndpoint in the Reporting tab > Software Deployment reports in the Package Version column.

For example:
• 8.4.295.1234.1234 - Shows a patch version.
• 8.4.295 - Shows a package version without a patch.

After a full version upgrade, the new version shows without patch numbers.

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.

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. In the screen that shows, 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 credentials:

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.
AD Users and Groups for SmartConsole Authentication

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 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).

   =========== Certificate 0 ===========
   X509 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`


---

**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.

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**.

**Changes in Reporting**

From the **Reporting** tab > **Options** icon > **Export Report**, reports are now faster and only export 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: `$UEPMDIR/engine/conf/local.properties`
3. Find the line: `#emon.scheduler.time=9:55:00,10:55:00,15:33:00`
   - Delete the `#` from the line
   - Edit the times to show the hour when the reports will be created. Reports will be created each day at these times.
   - Make sure the line is in this format: `emon.scheduler.time=HH:mm:ss,HH:mm:ss,HH:mm:ss` with no spaces between the times and commas.
4. Find the line: `#emon.scheduler.max.reports=10`
   - Delete the `#` from the line
   - The number represents the maximum number of reports that can remain in the report directory. The oldest ones are overridden by newer ones. Optional: Edit the number.
   - Make sure the line is in this format: `emon.scheduler.max.reports=<number of reports to save>`.
5. Find the line: `#emon.scheduler.policyreport=true`
   - Delete the `#` from the line
   - Make sure the line is in this format: `emon.scheduler.policyreport=true`
6. Create a new folder in `$FWDIR/conf/SMC_Files/uepm/reports/`. Run:
   ```bash
   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 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.

---

**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 Common 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... 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.

Upgrading Windows Versions

- You cannot upgrade to Windows 8 or 8.1 from Windows 7 or lower while an Endpoint Security client is installed.
- To upgrade from Windows 8 to 8.1 with a client that has the Full Disk Encryption blade, use the procedures in sk99064 http://supportcontent.checkpoint.com/solutions?id=sk99064.

To upgrade Windows from 7 or XP to version 8 or 8.1:

1. Uninstall the Endpoint Security client.
2. Upgrade the Windows version.
3. Install the Endpoint Security client.
## 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>
<tbody>
<tr>
<td>01574755</td>
<td>In Surface Pro2 (Windows 8 64bit) with Type Cover 2, the cursor movement at preboot screen is strange.</td>
</tr>
<tr>
<td>01574771</td>
<td>Windows RE tools area is not encrypted.</td>
</tr>
<tr>
<td>01574774</td>
<td>You cannot type &quot;_&quot; using Type Cover 2.</td>
</tr>
<tr>
<td>00673418</td>
<td>It is not possible to unlock FAT32 and FAT volumes in Full Disk Encryption Drive Slaving Utility on BIOS systems. You will not be able to access the files, even if you authenticate to the volumes.</td>
</tr>
</tbody>
</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. |
| 00674375   | Installing Full Disk Encryption on Dell Latitude E series 3*50, 5*50 and 7*50 in BIOS mode causes a Green Screen or an “SA not found error”. |
| 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). |

### 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>
</tbody>
</table>
### Known Limitations

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01463737</td>
<td>The Common Client Settings policy enforced is the last one downloaded from the server.</td>
</tr>
<tr>
<td>01646152</td>
<td>Net 2.0 service pack 2 must be installed on client computers before Endpoint Security Client installation.</td>
</tr>
<tr>
<td></td>
<td>Only FDE and ME 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>01447512</td>
<td>For environments with High Availability and Remote Help Servers that are synchronized with Automatic Synchronization: To restore Endpoint Security Data with the migrate import command, contact Check Point support with issue number 01447512.</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></td>
<td>R77.20 Jumbo HF installation cannot be installed on the top of EP5.6.</td>
</tr>
<tr>
<td>01688251</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>00673975</td>
<td>On 32-bit computers: When Media Encryption is installed on a computer with SecureBoot enabled, Windows will be not start and will go into repair mode. Disable SecureBoot for Media Encryption to work correctly.</td>
</tr>
<tr>
<td>01658984</td>
<td>When encrypting a DVD-RW or CD-RW media, the media session closes after the encryption finishes. To add more data, erase the encrypted media and start over. DVD-RW disk becomes read only after encryption with ME.</td>
</tr>
</tbody>
</table>
Resolved Issues

<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>

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 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>

Resolved Issues

These issues are resolved in this release:

Full Disk Encryption

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00673896</td>
<td>If the domain selection in the Pre-boot authentication is dropped down, the Tab key (or Shift+tab) does not move to the next selection.</td>
</tr>
<tr>
<td>00673685</td>
<td>If the password synchronization fails, the messages in the client UI are not clear.</td>
</tr>
<tr>
<td>00674304</td>
<td>If a USB device is inserted while a computer boots, then the eject of the device in Windows fails.</td>
</tr>
<tr>
<td>00674043</td>
<td>Pre-boot input on a virtual keyboard can sometimes result in multiple keys entered instead of just one. This occurs on Lenovo Helix.</td>
</tr>
<tr>
<td>00674038</td>
<td>The UseRec.exe tool fails to load some recovery files.</td>
</tr>
<tr>
<td>00674232</td>
<td>Single Sign-on does not work correctly after a shut down on Surface Pro 3. This is because of the Connected Standby feature on the Surface Pro 3.</td>
</tr>
<tr>
<td>00674163</td>
<td>The Pre-boot login screen on Surface Pro 3 is too small.</td>
</tr>
<tr>
<td>00674102</td>
<td>User acquisition does not work for users who had a Legacy Token that was upgraded.</td>
</tr>
</tbody>
</table>
### Resolved Issues

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00674091</td>
<td>On some computers Pre-boot Bypass does not work when the Hardware Hash feature is configured.</td>
</tr>
<tr>
<td>00674160</td>
<td>The computer might hang when the when pre-boot screensaver starts on Surface Pro 3.</td>
</tr>
<tr>
<td>00673822</td>
<td>To install Full Disk Encryption on an HP ElitePad 1000 G2:</td>
</tr>
<tr>
<td></td>
<td>1. Make sure that the BIOS/Firmware version of the HP ElitePad 1000 G2 is 01.30 A, released 4 December 2014. If you have a different version installed, download this version.</td>
</tr>
<tr>
<td></td>
<td>2. Create the REG_SZ registry key \HKLM\SOFTWARE\Wow6432Node\CheckPoint\Endpoint Security\Full Disk Encryption\UEFIInstallationMode and set the value to NVRAM.</td>
</tr>
<tr>
<td></td>
<td>3. Deploy the Full Disk Encryption package.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The UEFIInstallationMode registry value is a string that might have the value BOOTMGFW. The value can also be NVRAM which will create a BootEntryXXXX NVRAM variable and set it accordingly in the related BootOrder variable so that Full Disk Encryption starts first.</td>
</tr>
</tbody>
</table>

### Active Directory

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01675947</td>
<td>LDAP login for Security Management Servers supports nested AD groups. If the AD has multiple levels of nested groups, LDAP login may impact the performance of the AD server. Use the Microsoft hotfix for Windows Server 2003 <a href="https://support.microsoft.com/en-us/kb/914828">https://support.microsoft.com/en-us/kb/914828</a> to improve the performance for the underlying LDAP query.</td>
</tr>
</tbody>
</table>

### Media Encryption & Port Protection

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01502988</td>
<td>User permissions are not properly activated when using the Windows User Switch feature. If you log on with user A first and then switch users (with Windows user switch) to user B, user B gets the permissions that user A has configured.</td>
</tr>
<tr>
<td>01502994</td>
<td>In the Media Encryption Offline Utility, the local time is used when changing timestamp files. This can cause issues when working with NTFS, which stores time using UTC time. Resolution: When handling files from NTFS, UTC time is used.</td>
</tr>
</tbody>
</table>
## Resolved Issues

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01568614</td>
<td>If you have a Media Encryption encrypted USB device that is formatted with NTFS, you must run a dependency installer to be able to read the files with the Media Encryption Offline Tool.</td>
</tr>
<tr>
<td></td>
<td>Resolution: The drivers required to read the files with the offline tool are easily installed with the Media Encryption Offline Tool itself.</td>
</tr>
<tr>
<td></td>
<td>• To install: Run the Media Encryption Offline Tool with the -i argument.</td>
</tr>
<tr>
<td></td>
<td>• To uninstall: Run the offline unlock tool with the -u argument.</td>
</tr>
<tr>
<td></td>
<td>You must install and uninstall the drivers with administrator privileges.</td>
</tr>
</tbody>
</table>

### Offline Mode

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00674156</td>
<td>The local Work folder for pushing update policies is protected. Files cannot be deleted, changed or copied to this location. Drag and drop files to add them to the Work folder.</td>
</tr>
</tbody>
</table>

### Management

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01447512</td>
<td>You must enable Endpoint Security Management on the Management Server before you restore Endpoint Security data with the migrate import command.</td>
</tr>
<tr>
<td></td>
<td>Revert to snapshot is not supported.</td>
</tr>
</tbody>
</table>