HARMONY

15 May 2025

HARMONY ENDPOINT SERVER

R81.20

Administration Guide

CHECK POINT™

Check Point Copyright Notice

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.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R81.20 Harmony Endpoint Server Administration Guide

For more about this release, see the R81.20 home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Patent Notice

Check Point Harmony Endpoint Server is protected by the following patents in the United States and elsewhere.
This page is intended to serve as notice under 35 U.S.C. § 287(a):
US7,340,770, US7,540,013, US7,546,629, US7,627,896, US7,725,737,US7,788,726, US7,930,744, US8,074,277, US8,136,149, US8,136,155,US8,161,188, US8,200,818, US8,281,114, US8,370,934, US8,769,268,US8,843,993, US9,208,317, US9,298,921, US9,356,945, US9,536,090,US9,686,307, US9,888,032, US10,050,995, US10,193,906, US10,291,634,US10,382,493, US10,440,036, US10,462,160, US10,467,407, US10,511,616,US10,567,395, US10,728,266, US10,880,316, US10,972,488, US11,165,820,US11,606,375, US11,960,606

Note - SmartEndpoint will reach its End of Support (EOS) on December 31, 2025. You can access SmartEndpoint functionality in the Harmony Endpoint Web Management Console. Refer to sk183410.

Revision History

Date	Description
21 April 2025	Removed the content related to Capsule Docs, which has already reached End of Support (EOS) as of December 2024.
19 November 2024	Added *"Supported Operating Systems for the Endpoint Client" on page 49*.
4 September 2023	Added *"Smart App Control" on page 414* for Windows 11.
11 January 2023	Added new Push Operations. See *" Performing Push Operations" on page 69*.
18 November 2022	Initial release of the document.

Table of Contents

Introduction to Endpoint Security

Check Point endpoint security includes data security, network security, advanced threat prevention, forensics, and remote access VPN solutions. It offers simple and flexible security administration: The entire endpoint security suite can be managed centrally using a single management console.

Managing the Security of Users, Not Just Machines

One user may have multiple computers and some computers may have multiple users. Therefore, the Security Policies for some Endpoint Security components are enforced for each user, and some are enforced on computers.

Organization-Centric model

You can import users and computers to the **Endpoint Security Management Server**, which uses your organization's existing hierarchy to provide a graphical tree of endpoints computers. You then define software deployment and security policies centrally for all nodes and entities, making the assignments as global or as granular as you need.

Policy-centric Model

You can predefine security policies before setting up the organization. The Endpoint Security Management Server interface provides a granular view of all the Endpoint Security policies, grouped by the components they configure.

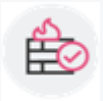
You create and assign policies to the root node of the organizational tree as a property of each Endpoint Security component. Policies can be deployed one by one or all together. Because different groups, networks, OUs, computers, and users have different security needs, you can configure different components accordingly.

Endpoint Security Client

You can define policies in SmartEndpoint for the Endpoint Security client components. The Endpoint Security client is available on Windows and Mac.

Note - SmartEndpoint will reach its End of Support (EOS) on December 31, 2025. You can access SmartEndpoint functionality in the Harmony Endpoint Web Management Console. Refer to sk183410.

These are the Endpoint Security components that are available on Windows:

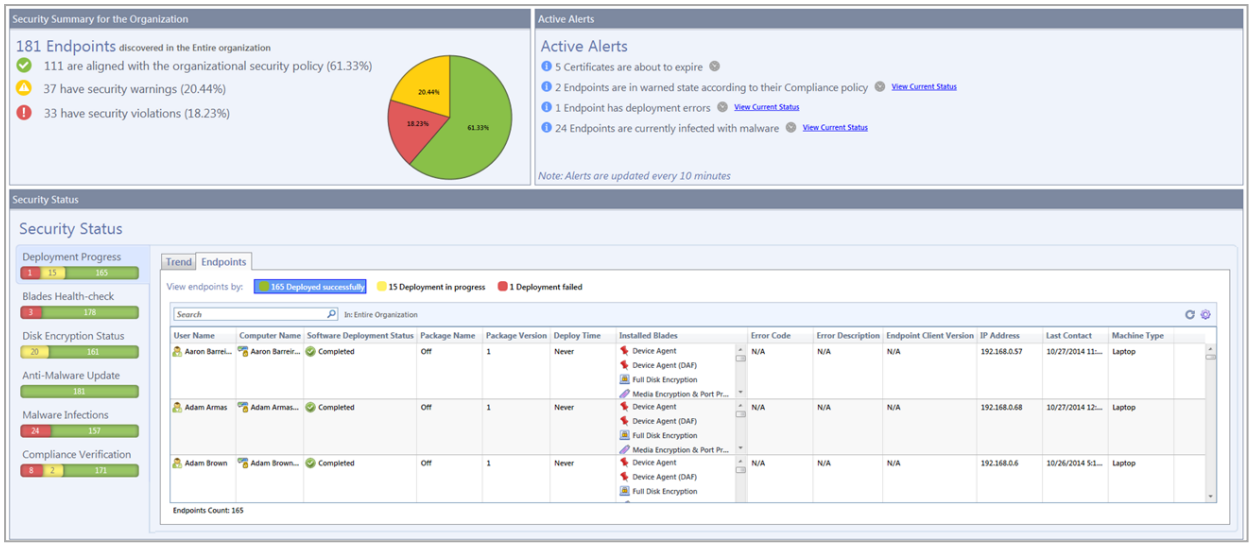
Component	Description
Compliance 	Allows you to enforce endpoint compliance on multiple checks before users log into the network. You can check that the: ■ appropriate endpoint security components are installed ■ correct OS service pack are installed on the endpoint ■ only approved applications are able to run on the endpoint ■ appropriate anti-malware product and version is running on the endpoint.
Anti-Malware 	Protects clients from known and unknown viruses, worms, Trojan horses, adware, and keystroke loggers.
Media Encryption and Media Encryption & Port Protection 	Protects data stored on the computers by encrypting removable media devices and allowing tight control over computers' ports (USB, Bluetooth, and so on).
Firewall and Application Control 	Defines the topology of the organizational network, separating it into Trusted and Internet domains. Blocks or allows network traffic based on attributes of network connections. Controls network access on a per-application basis, letting you restrict application access by zone and direction.
Full Disk Encryption 	Combines Pre-boot protection, boot authentication, and strong encryption to make sure that only authorized users are given access to information stored on desktops and laptops. Manages: ■ How a Full Disk Encryption user logs in to the computer ■ How failed logins are handled ■ Password security ■ Access to remote help
Remote Access VPN 	Provide secure, seamless access to corporate networks remotely, over IPsec VPN.

Component	Description
URL Filtering 	Lets organizations control access to web sites by category, user or group.
Harmony Endpoint Anti-Bot 	Detects bot-infected machines and blocks bot C&C communication to prevent bot damage. Provides detailed information about the device affected by the bot activity, about the bot process itself, and other relevant information.
Harmony Endpoint Anti-Ransomware, Behavioral Guard and Forensics 	Prevents ransomware attacks. Monitors files and the registry for suspicious processes and network activity. Analyzes incidents reported by other components.
Harmony Endpoint Threat Extraction, Emulation and Anti-Exploit 	Threat Extraction quickly delivers safe files while the original files are inspected for potential threats. Threat Emulation sends files on the endpoint computer to a sandbox for emulation to detect evasive zero-day attacks.

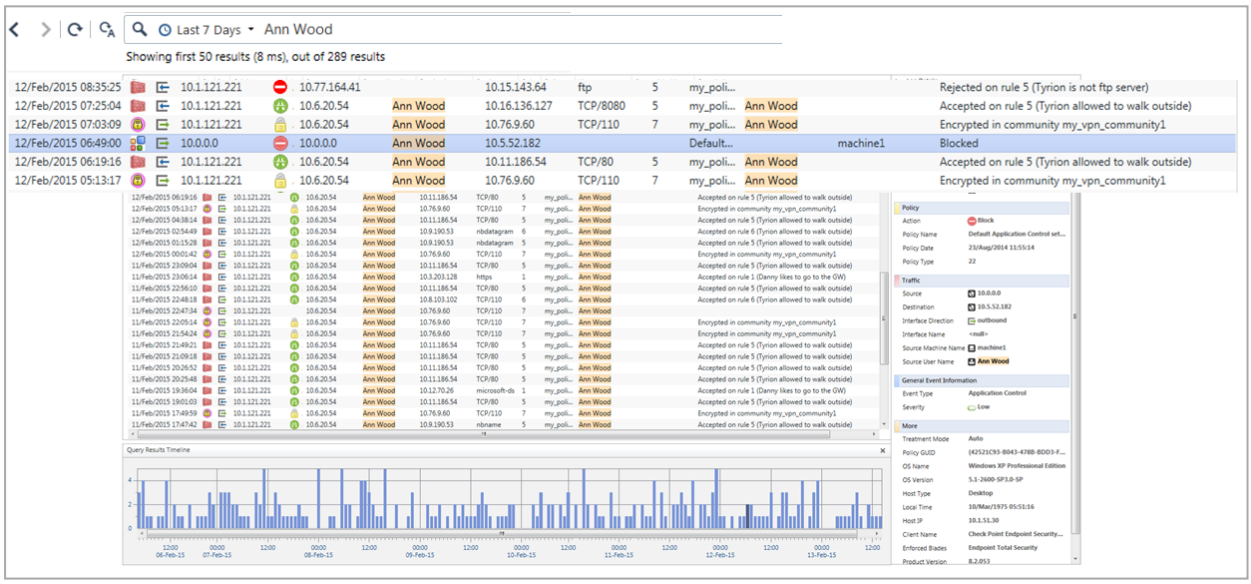
Centralized Monitoring

The Endpoint Security Management Server provides reports for the whole system as well as individual users and computers.

- **General status reports** can be viewed in the SmartEndpoint GUI client. You can monitor Endpoint Security client connection status, compliance to security policy status, information about security events, and more.



- **Historical data for clients and servers** can be viewed in the **Logs** tab of the SmartConsole **Logs & Monitor** view.

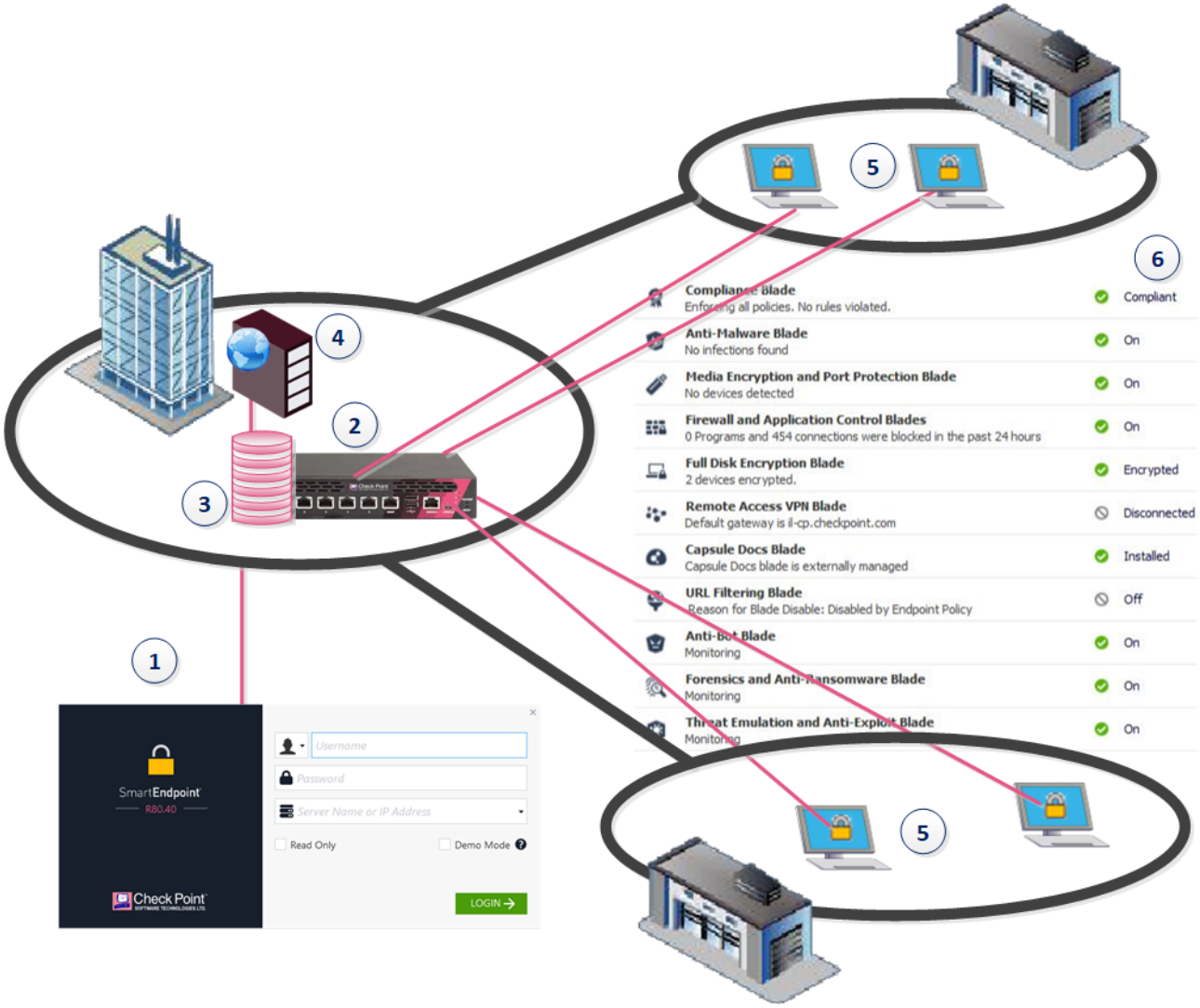


Centralized Deployment

Deployment in the Endpoint Security Management Server lets you control specific components and Endpoint Security versions installed on the protected end-user computers.

Endpoint Security Architecture

An Endpoint Security environment includes the SmartEndpoint console, Endpoint Security Management Server, and Endpoint Security clients. It is integrated with the Check Point Security Management and SmartConsole.



Endpoint Security Management Server

	Item	Description
1	**Active Directory Server**	The repository of the user information of the organization. (Not part of the Endpoint Security Management Server.)

	Item	Description
2	**Endpoint Security Management Server**	Includes the Endpoint Security policy management and databases. It communicates with endpoint clients to update their components, policies, and protection data. The **Endpoint Security Database** holds policies that enforce security on endpoint clients, user and computer objects, licensing, and Endpoint monitoring data. Also contains the **Directory Scanner**, that gets the structure and contents of the **Active Directory Server** for directory-based policy assignment. **Note** - The term Endpoint Security Management Server refers to all Endpoint Security Servers in the environment. This includes Endpoint Security Management Servers and the (optional) Endpoint Policy Servers.
3	**SmartEndpoint**	A Check Point SmartConsole application to deploy, monitor and configure Endpoint Security clients and policies. Install on the **Endpoint Security Management Server** or on a Windows computer that supports the client installation.

Endpoint Security Clients

	Item	Description
4	**Endpoint Security Clients**	Application installed on end-user computers to monitor security status and enforce security policies.
5	**Endpoint Security components**	The components deployed on the endpoint client. You can install any or all of these components from the **Endpoint Security Management Server**.

For Endpoint Security Server and Endpoint Security Client requirements, see the *R81.20 Release Notes*.

Optional Endpoint Security Elements

To make sure that your Endpoint Security system runs efficiently and without unnecessary down time, you can also include these optional elements in your system architecture:

	Item	Description
6	**Secondary Endpoint Security Management Server**	One additional Endpoint Security Management Server for High Availability. This makes sure that a backup server is available if the primary server is down.
7	**Endpoint Policy Servers**	Endpoint Policy Servers improve performance in large environments by managing most communication with the Endpoint Security clients. Managing the Endpoint Security client communication decreases the load on the Endpoint Security Management Server, and reduces the bandwidth required between sites. The Endpoint Policy Server handles heartbeat and synchronization requests, Policy downloads, Anti-Malware updates, and Endpoint Security client logs.

Endpoint Security Server and Client Communication

Endpoint Security functionality is based on secure communication between all Endpoint Security servers and clients.

Endpoint Security operations are implemented by different services on the Endpoint Security Management Server, Endpoint Policy Servers, SmartEndpoint console, and Endpoint Security clients.

Important - Make sure that

- HTTP (TCP/80) and HTTPS (TCP/443) services and ports are allowed by Firewall or Application Control rules.
- There is routing between the Endpoint Security elements.

SmartEndpoint Console and Server to Server Communication

Communication between these elements uses the Check Point Secure Internal Communication (SIC) service. The elements authenticate each other using certificates. HTTPS (TCP/443) is used for sending events, for SmartEvent Views and Reports, from the Endpoint Policy Server to Primary Management.

Service (Protocol/Port)	Communication	Notes
SIC (TCP/18190 - 18193)	SmartEndpoint console to Endpoint Security Management Servers	
	Endpoint Policy Server to Endpoint Security Management Servers	Endpoint Policy Server distribute and reduce the load of client-server communication between the clients and the Endpoint Security Management Server.
SIC (TCP/18221)	Endpoint Secondary to Primary Management	
HTTPS (TCP/443)	Endpoint Policy Server to Primary Management	Used for sending monitoring events.

Client to Server Communication

These services are used by the client to communicate with the Endpoint Policy Server or the Endpoint Security Management Server.

The client is always the initiator of the connections.

Service (Protocol/Port)	Communication	Notes
HTTPS (TCP/443)	Most communication is over HTTPS TLSv1.2 encryption.	These are two examples: ■ Endpoint registration ■ New file encryption key retrieval
	Policy downloads	The policy files themselves are encrypted with AES.
	Heartbeat	A periodic client connection to the server. The client uses this connection to inform the server about changes in the policy status and compliance. You can configure the *Heartbeat interval*. See *"The Heartbeat Interval" on the next page*
	Application Control queries	These are queries for the reputation of unknown applications.
	Log uploads	These connections send logs to the server.
	For more sensitive services, the payload is encrypted using a proprietary Check Point protocol.	These are the encrypted sensitive services: ■ Full Disk Encryption Recovery Data Upload ■ Media Encryption & Port Protection Key Exchange ■ Full Disk Encryption User Acquisition & User credentials.
HTTPS (TCP/80)	Anti-Malware signature updates	Verification is done by the engine before loading the signatures, and during the update process.
HTTPS (TCP/443)	Client package downloads	The packages are signed and verified on the client before being installed.

The Heartbeat Interval

Endpoint clients send "heartbeat" messages to the Endpoint Security Management Server to check the connectivity status and report updates. The time between heartbeat messages is known as the *heartbeat interval.*

Note - The default heartbeat interval is 60 seconds.
A shorter heartbeat interval can cause additional load on the management. A longer heartbeat interval may lead to less up-to-date logs and reports.

The endpoint computer Compliance state is updated at each heartbeat. The heartbeat interval also controls the time that an endpoint client is in the **About to be restricted** state before it is restricted.

It is possible to create restricted policies that will automatically be enforced once the endpoint client enters a restricted state

To configure the heartbeat interval and out-of-compliance settings:

1. Click **Manage > Endpoint Connection Settings**.

   The **Connection Settings Properties** window opens.
2. In the **Connection Settings** section, set the **Interval between client heartbeats**.
3. In the **Out-Of-Compliance** section, configure when a client is restricted. Configure the number of heartbeats in **Client will restrict non compliant endpoint after**. The default is 5 heartbeats.
4. Click **OK**.

SHA-256 Certificate Support

For R80 and higher clean installations, the management certificate is encrypted with SHA-256 encryption by default. In R77.X and lower environments, or upgrades from those versions, SHA-256 is not supported for the Root CA. You can use SHA-256 for renewed certificates after the previous certificate expires. See sk103840 for more information.

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:

On each Endpoint Security server:

1. Run:

   ```
   cpstop
   ```

2. Edit:

   ```
   $UEPMDIR/apache/conf/ssl.conf
   ```

3. Change the value of the `SSLProtocol` attribute

   from:

   ```
   SSLProtocol +TLSv1 +TLSv1.2
   ```

   to:

   ```
   SSLProtocol TLSv1.2
   ```

4. Save the changes.

5. Run:

   ```
   cpstart
   ```

External PKI Certificates for Client-Server Communication

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. 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** - Full Disk Encryption that is installed on the client uses this certificate to work with the Remote Help server for password recovery.
- **Unlock on LAN** - Full Disk Encryption that is 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 External PKI 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. From the Menu, go to **Manage** > **Certificate Management**.

   The **Endpoint Security Management** window opens.
3. Click **Import**.

   The **Import Certificate Wizard** opens.
4. On the **Import Certificate** page:

a. Select the certificate type.

b. Insert the certificate file. You can drag and drop the file into the window or navigate to it from the folder icon.

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 opens:

   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 Certificate** page opens:

   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**.

9. Click **Close**.

Installing CA Certificates on Clients

To install a CA certificate:

1. Open **SmartEndpoint**.

2. In the **Users and Computers** tab, in the **Global Actions** section, click **Push Operation**.

   The **Create Push Operation** wizard opens.

3. At the top, select **Client Settings**.

4. Select **Push CA Certificate** and click **Next**.
5. Select the computers to push the certificate to.
6. Click **Next**.
7. Click **Manage**.
8. Select the certificate and click **Assign**.
9. **Optional:** Enter a descriptive **Comment**.
10. Click **Next**.
11. 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 finished**.
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:

1. In the **Offline Group Settings**, select **Select existing certificate**.
2. Click **Manage** and select the certificate from the list or click **Import** to get the certificate.
3. Click **Assign**.
4. Continue with the **New Offline Group** wizard, as described in Configuring an Offline Group.

When editing an existing offline group:

1. Go to **Group Details** and click **Edit**.
2. Click **Manage** and select the specific certificate.
3. Click **OK**.

Monitoring Certificates

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.

Connection Port to Services on an Endpoint Security Management Server

Background

Important:

SSL connection ports on Security Management Servers R81 and higher

- A Security Management Server listens to SSL traffic for *all* services on the TCP port **443** in these cases:
  - If you performed a clean installation of a Security Management Server and enabled the **Endpoint Policy Management**Software Blade.
  - If you upgraded a Security Management Server with disabled **Endpoint Policy Management** Software Blade to and enabled this Software Blade after the upgrade.

  In these cases, when **Endpoint Security** SSL traffic arrives at the TCP port 443, the Security Management Server automatically redirects it (internally) to the TCP port 4434.

Service	URL and Port
Gaia Portal	`https://<IP Address of Gaia Management Interface>`
SmartView Web Application	`https://<IP Address of Management Server>/smartview/`
Management API Web Services (see *Check Point Management API Reference*)	`https://<IP Address of Management Server>/web_api/<command>`

- If you upgraded a Security Management Server with enabled **Endpoint Policy Management** Software Blade to , then the SSL port configuration *remains* as it was in the previous version, from which you upgraded:

- A Security Management Server listens to Endpoint Security SSL traffic on the TCP port 443
- A Security Management Server listens to SSL traffic for *all other* services on the TCP port 4434:

Service	URL and Port
Gaia Portal	`https://<IP Address of Gaia Management Interface>:4434`
SmartView Web Application	`https://<IP Address of Management Server>:4434/smartview/`
Management API Web Services (see *Check Point Management API Reference*)	`https://<IP Address of Management Server>:4434/web_api/<command>`

In R81 and higher, an administrator can manually configure different TCP ports for the Gaia Portal (and other services) and Endpoint Security - **443** or **4434**. For the applicable procedures, see .

For the applicable procedures, see the *R81 Harmony Endpoint Security Server Administration Guide* > Chapter *Endpoint Security Architecture* > Section *Connection Port to Services on an Endpoint Security Management Server*.

In R81 and higher, an administrator can manually configure different TCP ports for the Gaia Portal (and other services) and Endpoint Security - **443** or **4434**. See the applicable procedures below.

SSL connection ports on Security Management Servers R80.40 and lower

- When you enable the **Endpoint Policy Management** Software Blade on a Security Management Server, the SSL connection port to these services automatically changes from the default TCP port **443** to the TCP port **4434**:

- **Gaia Portal**

Configuration	URL and Port
Default	`https://<IP Address of Gaia Management Interface>`
New	`https://<IP Address of Gaia Management Interface>:4434`

- **SmartView Web Application**

Configuration	URL and Port
Default	`https://<IP Address of Management Server>/smartview/`
New	`https://<IP Address of Management Server>:4434/smartview/`

- **Management API Web Services** (see *Check Point Management API Reference*)

Configuration	URL and Port
Default	`https://<IP Address of Management Server>/web_api/<command>`
New	`https://<IP Address of Management Server>:4434/web_api/<command>`

- When you disable the **Endpoint Policy Management** Software Blade on a Security Management Server, the SSL connection port automatically changes back to the default TCP port **443**.

Procedures

Possible configuration scenarios are:

Scenario	Gaia Portal Certificate	Gaia Portal Listening Port	Endpoint Security Listening Port
1	Self-signed SSL certificate	443	4434

Scenario	Gaia Portal Certificate	Gaia Portal Listening Port	Endpoint Security Listening Port
2	External SSL certificate	443	4434
3	Self-signed SSL certificate	4434	443
4	External SSL certificate	4434	443

Scenario 1 - Gaia Portal uses the default self-signed SSL certificate, Gaia Portal listens on TCP port 443, and Endpoint Security listens on TCP port 4434

1. Connect to the command line on the Endpoint Security Management Server.
2. Log in to the Expert mode.
3. Modify the `$UEPMDIR/apache/conf/ssl.conf` file:
   a. Back up the current file:
   ```
   cp -v $UEPMDIR/apache/conf/ssl.conf{,_BKP}
   ```
   b. Edit the current file:
   ```
   vi $UEPMDIR/apache/conf/ssl.conf
   ```
   c. Configure this value in the "`Listen`" directive:
   ```
   Listen  0.0.0.0:4434
   ```
   d. In the "`SSL Virtual Host Context`" section, configure this value in the "`VirtualHost`" directive:
   ```
   <VirtualHost _default_:4434>
   ```
   e. Save the changes in the file and exit the editor.
4. Modify the `/web/templates/httpd-ssl.conf.templ` file:

a. Back up the current file:

```
cp -v /web/templates/httpd-ssl.conf.templ{,_BKP}
```

b. Edit the current file:

```
vi /web/templates/httpd-ssl.conf.templ
```

c. In the "`Pass Phrase Dialog`" section, configure this value in the "`SSLPassPhraseDialog`" directive:

```
SSLPassPhraseDialog "exec:/opt/CPuepm-
R81.20/apache/bin/SSLPassPhraseDialog"
```

d. In the "`Server Certificate`" section, configure this value in the "`SSLCertificateFile`" directive:

```
SSLCertificateFile "/opt/CPuepm-
R81.20/engine/conf/ssl/sic_cert.pem"
```

e. In the "`Server Private Key`" section, configure this value in the "`SSLCertificateKeyFile`" directive:

```
SSLCertificateKeyFile "/opt/CPuepm-
R81.20/engine/conf/ssl/sic_cert-key.pem"
```

f. In the "`Server Certificate Chain`" section, configure this value in the "`SSLCertificateChainFile`" directive:

```
SSLCertificateChainFile "/opt/CPuepm-
R81.20/engine/conf/ssl/root_sic_cert.pem"
```

g. Save the changes in the file and exit the editor.

5. Configure the SSL port to 443 in the Gaia database.

   Run these two commands:

```
dbset httpd:ssl_port 443
dbset :save
```

6. Generate the Apache configuration. Run:

```
$UEPMDIR/system/install/gaia_apache_conf_regenerate
```

7. Restart Check Point services. Run:

```
cpstop && cpstart
```

Scenario 2 - Gaia Portal uses an external SSL certificate, Gaia Portal listens on TCP port 443, and Endpoint Security listens on TCP port 4434

1. Import and install the certificates:
   a. Obtain the **CA** certificate that generated the custom SSL certificate for the Gaia Portal.
   b. Import the applicable **CA** certificate on the Endpoint Security Management Server.

      Follow *"Importing External PKI Certificates" on page 30*.
   c. Import the new Gaia Portal **SSL** certificate on the Endpoint Security Management Server.

      Follow *"Importing External PKI Certificates" on page 30*.
   d. Install the new **CA** certificate on Endpoint Clients.

      Follow *"Installing CA Certificates on Clients" on page 31*.
   e. Install the new Gaia Portal **SSL** certificate on the Endpoint Security Management Server.

      Follow *"Installing SSL Certificates on Servers" on page 32*.
2. Connect to the command line on the Endpoint Security Management Server.
3. Log in to the Expert mode.
4. Modify the `$UEPMDIR/apache/conf/ssl.conf` file:
   a. Back up the current file:

      ```
      cp -v $UEPMDIR/apache/conf/ssl.conf{,_BKP}
      ```
   b. Edit the current file:

      ```
      vi $UEPMDIR/apache/conf/ssl.conf
      ```
   c. Configure this value in the "`Listen`" directive:

      ```
      Listen  0.0.0.0:4434
      ```

d. In the "`SSL Virtual Host Context`" section, configure this value in the "`VirtualHost`" directive:

```
<VirtualHost _default_:4434>
```

e. Save the changes in the file and exit the editor.

5. Modify the `/web/templates/httpd-ssl.conf.templ` file:

a. Back up the current file:

```
cp -v /web/templates/httpd-ssl.conf.templ{,_BKP}
```

b. Edit the current file:

```
vi /web/templates/httpd-ssl.conf.templ
```

c. In the "`Pass Phrase Dialog`" section, configure this value in the "`SSLPassPhraseDialog`" directive:

```
SSLPassPhraseDialog "exec:/opt/CPuepm-
R81.20/apache/bin/SSLPassPhraseDialog"
```

d. In the "`Server Certificate`" section, configure this value in the "`SSLCertificateFile`" directive:

```
SSLCertificateFile "/opt/CPuepm-
R81.20/engine/conf/ssl/sic_cert.pem"
```

e. In the "`Server Private Key`" section, configure this value in the "`SSLCertificateKeyFile`" directive:

```
SSLCertificateKeyFile "/opt/CPuepm-
R81.20/engine/conf/ssl/sic_cert-key.pem"
```

f. In the "`Server Certificate Chain`" section, configure this value in the "`SSLCertificateChainFile`" directive:

```
SSLCertificateChainFile "/opt/CPuepm-
R81.20/engine/conf/ssl/root_sic_cert.pem"
```

g. Save the changes in the file and exit the editor.

6. Configure the SSL port to 443 in the Gaia database.

Run these two commands:

```
dbset httpd:ssl_port 443
dbset :save
```

7. Generate the Apache configuration. Run:

```
$UEPMDIR/system/install/gaia_apache_conf_regenerate
```

8. Restart Check Point services. Run:

```
cpstop && cpstart
```

Scenario 3 - Gaia Portal uses the default self-signed SSL certificate, Gaia Portal listens on TCP port 4434, and Endpoint Security listens on TCP port 443

1. Connect to the command line on the Endpoint Security Management Server.
2. Log in to the Expert mode.
3. Modify the `$UEPMDIR/apache/conf/ssl.conf` file:
   a. Back up the current file:

```
cp -v $UEPMDIR/apache/conf/ssl.conf{,_BKP}
```

   b. Edit the current file:

```
vi $UEPMDIR/apache/conf/ssl.conf
```

   c. Configure this value in the "`Listen`" directive:

```
Listen  0.0.0.0:443
```

   d. In the "`SSL Virtual Host Context`" section, configure this value in the "`VirtualHost`" directive:

```
<VirtualHost _default_:443>
```

   e. Save the changes in the file and exit the editor.
4. Modify the `/web/templates/httpd-ssl.conf.templ` file:

a. Back up the current file:

```
cp -v /web/templates/httpd-ssl.conf.templ{,_BKP}
```

b. Edit the current file:

```
vi /web/templates/httpd-ssl.conf.templ
```

c. In the "`Pass Phrase Dialog`" section, configure this value in the "`SSLPassPhraseDialog`" directive:

```
SSLPassPhraseDialog exec:/bin/passphrase_xlate
```

d. In the "`Server Certificate`" section, configure this value in the "`SSLCertificateFile`" directive:

```
SSLCertificateFile /usr/local/apache2/conf/server.crt
```

e. In the "`Server Private Key`" section, configure this value in the "`SSLCertificateKeyFile`" directive:

```
SSLCertificateKeyFile
/usr/local/apache2/conf/server.key
```

f. In the "`Server Certificate Chain`" section, configure this value in the "`SSLCertificateChainFile`" directive:

```
SSLCertificateChainFile /usr/local/apache2/conf/server-
ca.crt
```

g. Save the changes in the file and exit the editor.

5. Configure the SSL port to 4434 in the Gaia database.

   Run these two commands:

```
dbset httpd:ssl_port 4434
dbset :save
```

6. Generate the Apache configuration. Run:

```
$UEPMDIR/system/install/gaia_apache_conf_regenerate
```

7. Restart Check Point services. Run:

```
cpstop && cpstart
```

Scenario 4 - Gaia Portal uses an external SSL certificate, Gaia Portal listens on TCP port 4434, and Endpoint Security listens on TCP port 443

1. Import and install the certificates:
   a. Obtain the **CA** certificate that generated the custom SSL certificate for the Gaia Portal.
   b. Import the applicable **CA** certificate on the Endpoint Security Management Server.

      Follow *"Importing External PKI Certificates" on page 30*.
   c. Import the new Gaia Portal **SSL** certificate on the Endpoint Security Management Server.

      Follow *"Importing External PKI Certificates" on page 30*.
   d. Install the new **CA** certificate on Endpoint Clients.

      Follow *"Installing CA Certificates on Clients" on page 31*.
   e. Install the new Gaia Portal **SSL** certificate on the Endpoint Security Management Server.

      Follow *"Installing SSL Certificates on Servers" on page 32*.
2. Connect to the command line on the Endpoint Security Management Server.
3. Log in to the Expert mode.
4. Modify the `$UEPMDIR/apache/conf/ssl.conf` file:
   a. Back up the current file:

      ```
      cp -v $UEPMDIR/apache/conf/ssl.conf{,_BKP}
      ```
   b. Edit the current file:

      ```
      vi $UEPMDIR/apache/conf/ssl.conf
      ```
   c. Configure this value in the "`Listen`" directive:

      ```
      Listen  0.0.0.0:4434
      ```
   d. In the "`SSL Virtual Host Context`" section, configure this value in the "`VirtualHost`" directive:

      ```
      <VirtualHost _default_:4434>
      ```
   e. Save the changes in the file and exit the editor.

5. Modify the `/web/templates/httpd-ssl.conf.templ` file:
   a. Back up the current file:

   ```
   cp -v /web/templates/httpd-ssl.conf.templ{,_BKP}
   ```

   b. Edit the current file:

   ```
   vi /web/templates/httpd-ssl.conf.templ
   ```

   c. In the "`Pass Phrase Dialog`" section, configure this value in the "`SSLPassPhraseDialog`" directive:

   ```
   SSLPassPhraseDialog exec:/bin/passphrase_xlate
   ```

   d. In the "`Server Certificate`" section, configure this value in the "`SSLCertificateFile`" directive:

   ```
   SSLCertificateFile /usr/local/apache2/conf/server.crt
   ```

   e. In the "`Server Private Key`" section, configure this value in the "`SSLCertificateKeyFile`" directive:

   ```
   SSLCertificateKeyFile
   /usr/local/apache2/conf/server.key
   ```

   f. In the "`Server Certificate Chain`" section, configure this value in the "`SSLCertificateChainFile`" directive:

   ```
   SSLCertificateChainFile /usr/local/apache2/conf/server-
   ca.crt
   ```

   g. Save the changes in the file and exit the editor.
6. Configure the SSL port to 4434 in the Gaia database.

   Run these two commands:

   ```
   dbset httpd:ssl_port 4434
   dbset :save
   ```

7. Generate the Apache configuration. Run:

   ```
   $UEPMDIR/system/install/gaia_apache_conf_regenerate
   ```

8. Restart Check Point services. Run:

```
cpstop && cpstart
```

Supported Operating Systems for the Endpoint Client

Microsoft Windows

Microsoft Windows

Version	Editions	Supported starting from
11 LTSC (version 24H2)	Enterprise Pro	Endpoint Security Client E88.41 VPN Standalone Client E88.40
11 24H2	Enterprise Pro	Endpoint Security Client E88.41 VPN Standalone Client E88.40
11 23H2	Enterprise Pro	Endpoint Security Client E87.62 VPN Standalone Client E87.60
11 22H2	Enterprise Pro	Endpoint Security Client E86.70
11 21H2	Enterprise Pro	Endpoint Security Client E85.40
10 22H2	Enterprise Pro	EA support: Endpoint Security Client E86.80 GA support: Endpoint Security Client E87.00
10 LTSC (version 21H2)	Enterprise Pro	Endpoint Security Client E86.00
10 21H2	Enterprise Pro	Endpoint Security Client E86.00
10 21H1 (version 2103)	Enterprise Pro	Endpoint Security Client E85.00
10 20H2 (version 2009)	Enterprise Pro	Endpoint Security Client E85.00
10 20H1 (version 2004)	Enterprise Pro	Endpoint Security Client E85.00
10 19H2 (version 1909)	Enterprise Pro	Endpoint Security Client E85.00
10 19H1 (version 1903)	Enterprise Pro	Endpoint Security Client E85.00
10 LTSC (version 1809)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1809)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1803)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1709)	Enterprise Pro	Endpoint Security Client E85.00
10 LTSB (version 1607)	Enterprise Pro	Endpoint Security Client E85.00
8.1 Update 1	Enterprise Pro	Endpoint Security Client E85.00
7 SP1 Microsoft update KB3033929	Enterprise Professional	Endpoint Security Client E85.00

Notes:

- For existing Endpoint Security deployments, before upgrading your OS version, you must first upgrade the Endpoint Security Client to a version that supports the desired OS version based on the table above.
- For additional information on Windows 7 support, refer to sk164006.
- Windows Operating Systems are supported according to Check Point Client Support life cycles, also on Virtual Machines. However, there is no dedicated QA process for all possible variants of Windows. If you encounter a specific issue related to a different edition of a supported Windows OS version, Check Point will provide best-effort support through R&D assistance.

Microsoft Windows Server

Version	Editions	Supported starting from	Supported Features
2025 64-bit	All	E88.61	Anti-Bot and URL Filtering, Anti-Malware, Anti-Ransomware, Behavioral Guard and Forensics, Compliance and Posture, Firewall and Application Control, Media Encryption and Port Protection, Threat Emulation.
2022 64-bit	All	E85.40	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Media Encryption and Port Protection.
2019 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Media Encryption and Port Protection.
2016 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.
2012 R2 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.
2012 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.
2008 R2 32/64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.

Notes:

- To support Endpoint Compliance rules for Windows Server 2016 on versions older than R80.20, see sk122136.
- Windows Server CORE is not supported.
- If you install a client package with features that are not supported on the server, the installation succeeds but only the supported features are installed.
- The Anti-Exploit feature is supported starting from the 2016 64-bit version.

macOS

macOS Version	Supported starting from
macOS Sequoia (15)	EA support: Endpoint Security Client E88.70 GA support: Endpoint Security Client E89.00
macOS Sonoma (14)	EA support: Endpoint Security Client E87.60 GA support: Endpoint Security Client E87.70
macOS Ventura (13)	EA support: Endpoint Security Client E86.80 GA support: Endpoint Security Client E87.00
macOS Monterey (12)	EA support: Endpoint Security Client E85.30 GA support: Endpoint Security Client E86.20
macOS Big Sur (11)	Endpoint Security Client E84.30
macOS Catalina (10.15)	Endpoint Security Client E82.00

Notes:

- For existing Endpoint Security deployments, before upgrading your OS version, you must first upgrade the Endpoint Security Client to a version that supports the desired OS version based on the table above.
- Starting from E88.30, new features do not include support for macOS 10.15. Starting from E89.00, macOS 10.15 is not supported.

Linux

Distribution / OS Version	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Ubuntu 24.04 (64-bit)	✓	✓	–	–	–	–	–	–
Ubuntu 22.04 (64-bit) (Supported versions: 22.04 - 22.04.3)	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Ubuntu 20.04 (64-bit) (Supported versions: 20.04 - 20.04.6)	✓	✓	✓	✓	✓	–	–	–
Ubuntu 18.04* (64-bit) (Supported versions: 18.04 - 18.04.6)	✓	✓	✓	✓	✓	–	–	–
Ubuntu 16.04 (64-bit)	✓	✓	✓	✓	✓	–	–	–
Alma Linux 9 (64-bit) (Supported versions: 9.0 - 9.3)	✓	✓	✓	✓	✓	✓	–	–
Alma Linux 8 (64-bit) (Supported versions: 8.9 and 8.10)	✓	✓	✓	✓	✓	✓	–	–
Amazon Linux 2023	✓	–	–	–	–	–	–	–
Amazon Linux 2 (64-bit)	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
CentOS 8* (64-bit) (Supported versions: 8.0 - 8.5)	✓	✓	✓	✓	✓	–	–	–
CentOS 7 (64-bit) (Supported versions: 7.8 - and 7.9)	✓	✓	✓	✓	✓	–	–	–
Debian Linux 12 (64-bit) (Supported versions: 12.0 - 12.5)	✓	✓	–	–	–	–	–	–
Debian Linux 11* (64-bit)	✓	✓	✓	✓	✓	–	–	–
Debian Linux 10* (64-bit)	✓	✓	✓	✓	✓	–	–	–
Debian Linux 9* (64-bit)	✓	✓	✓	✓	✓	–	–	–
Fedora 39[1]	✓	✓	✓	✓	✓	–	–	–
Fedora 38[1]	✓	✓	✓	✓	✓	–	–	–
Fedora 37	✓	✓	✓	✓	✓	–	–	–
Fedora 36	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Fedora 35	✓	✓	✓	✓	✓	–	–	–
Fedora 34	✓	✓	✓	✓	✓	–	–	–
OpenSUSE 15.4 and OpenSUSE 15.5	✓	✓	✓	✓	✓	–	–	–
OpenSUSE 42.3	✓	✓	✓	✓	✓	–	–	–
Oracle Linux 8 (64-bit) (Supported versions: 8.0 - 8.10)	✓	✓	✓	✓	✓	✓	✓	✓
Oracle Linux 7.9 (64-bit)	✓	✓	✓	✓	✓	–	–	–
Red Hat Enterprise Linux (RHEL) 9 [1] (64-bit) (Supported versions: 9.0 - 9.5)	✓	✓	✓	✓	✓	✓	✓	✓
Red Hat Enterprise Linux (RHEL) 8 (64-bit) (Supported versions: 8.0 - 8.9)	✓	✓	✓	–	–	–	–	–

Distribution / OS Version	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Red Hat Enterprise Linux (RHEL) 8.10 (64-bit)	✓	✓	–	–	–	–	–	–
Red Hat Enterprise Linux (RHEL) 7 (64-bit) (Supported versions: 7.8 and 7.9)	✓	✓	✓	✓	✓	–	–	–
Rocky 8.10	✓	–	–	–	–	–	–	–
Rocky 9.5	✓	–	–	–	–	–	–	–
SUSE Linux Enterprise Server (SLES) 15 (64-bit) (Supported versions: 15SP2 and 15SP3)	✓	✓	✓	✓	✓	✓	✓	✓
SUSE Linux Enterprise Server (SLES) 12 (64-bit) (Supported versions: 12SP5)	✓	✓	✓	✓	✓	–	–	–

[1] Only Anti-Malware support.

Endpoint Security Licenses

This chapter includes license information for Endpoint Security Servers and Clients. All Endpoint Security licenses are physically installed on the Endpoint Security Management Server.

For information about the available licenses, see the Harmony Endpoint product catalog.

Endpoint Security Product Licenses

You need to have a license for:

- Every Endpoint Security client. The license is per-seat.
- The Endpoint Security Management Server.

Demo and Temporary Licenses

These demo and trial Endpoint Security licenses are available:

License type	Explanation
Trial License	A 30 day trial license is automatically installed when you install Endpoint Security. This license lets you use all Endpoint Security components for a limited number of endpoint client seats.
Evaluation	An 30-day evaluation license is available for specified components for a specified number of seats. You must deploy a management evaluation license and an Endpoint Security client evaluation license.
Product	You must purchase a Product license for each Endpoint Security component running on a client. Licenses can be purchased as a Subscription, a contract that is renewed annually, or a one-time purchase.

License Enforcement

License activity conforms to these conditions:

- You can add Endpoint Security licenses as required using one of these methods:
  - SmartConsole. See the *R81.20 Security Management Administration Guide*..
  - The Gaia Portal. See the *R81.20 Gaia Administration Guide*.
  - The `cplic` or `cpconfig` CLI commands. See the *R81.20 CLI Reference Guide*.

- You can remove a client license by resetting the client or deleting the client using SmartEndpoint. These licenses are returned to the license pool.
- Each client gets its Container and Endpoint Security component licenses from a pool of available licenses.
- If you have mixed licenses, for example Harmony Basic for Server and Harmony Advanced on Laptops, then each client gets a random license from the pool mixed licenses available.
- You can combine licenses to reach the total number of required clients.
- License validation occurs when the client sends a SYNC or heartbeat messages to the server.

Getting Licenses

This procedure assumes that you have a user account for the Check Point User Center, and that the necessary licenses and contracts are purchased.

To get the license for your Endpoint Security Management Server:

1. Log in to *Check Point User Center*.
2. Click **My Products** > **My Products Center**.

   The page shows the purchased licenses.

   Endpoint Security licenses have these parts in the SKU:

   - CPEP - Check Point Endpoint Security containers.
   - CPSB - Check Point component. If the macro string includes the -SUBSCR suffix, you must get and apply a contract for this feature. See *"Getting and Applying Contracts" on the next page*.
3. For each license:
   a. Click the license to open it.
   b. In the window that opens, click **License**.
4. Fill in the form that opens.
   - Make sure that **Version** is **R80 or higher**.
   - Make sure that the **IP Address** is the IP address of the Endpoint Security Management Server.
5. Click **License**.

   A window opens, showing the license data.

6. Save the license file.
7. Add your licenses using one of these methods:
   - SmartConsole. See the *R81.20 Security Management Administration Guide*..
   - The Gaia Portal. See the *R81.20 Gaia Administration Guide*.
   - The `cplic` or `cpconfig` CLI commands. See the *R81.20 CLI Reference Guide*.

Getting and Applying Contracts

If the license includes `-SUBSCR`, you must download the contract file and apply it to the server. If the Endpoint Security Management Server has Internet access, it automatically renews contracts. By default, the Endpoint Security Management Server looks for new contracts every two hours.

To change the default time interval:

1. Edit this file:

   ```
   $CPDIR/conf/downloads/dl_prof_CNTRCTMNGR.xml
   ```

2. Change the `<interval>` value as necessary.
3. Restart Check Point services:

   ```
   cpstop ; cpstart
   ```

To apply a contract manually:

1. Log in to *Check Point User Center*.
2. Click **Products**.
3. Select **Get Contracts File** in the drop-down menu at the right of the row.
4. In the window that opens, save the contract file and click **Open**.
5. Connect with SmartConsole to the Endpoint Security Management Server.
6. Click Menu > **SmartUpdate**.
7. Select **License & Contracts** > **Updated Contracts** > **From File**.
8. In the window that opens, browse to where you saved the contract file and click **Open**.

   The contract is applied to the Endpoint Security Management Server.

If the Endpoint Security Management Server does not have access to the Internet, prepare the contract file download from the User Center differently.

To download a contract to a different computer:

1. In the User Center, click **Products** > **Additional Services**.
2. Select the account of the contract.
3. Click **Email File** or **Download Now**.
4. When you have the contract file, move it to the Endpoint Security Management Server.
5. Use the `cplic` or `cpconfig` CLI commands. See the *R81.20 CLI Reference Guide*.

Configuring a Proxy for Internet Access

If the Endpoint Security Management Server requires a proxy to connect to the internet, configure the proxy details in SmartConsole.

To configure a proxy for the Endpoint Security Management Server:

1. Connect with SmartConsole to the Endpoint Security Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the Endpoint Security Management Server object.
4. Click **Network Management** > **Proxy**.
5. Select **Use custom proxy settings for this network object**.
6. Select **Use proxy server** and enter the URL and port.
7. Click **OK**.
8. **Install Database**.

License Status

You can see the status of container and component licenses in Endpoint Security Management Server on the **Reporting** tab > **Licenses Report**. This pane shows the total number of seats and seats in use. If the number of seats exceeds the number of licenses, you must add the number of licenses shown as **Insufficient Seats**.

The lower section of the report shows the details of each license including:

- License Name and status
- Endpoint Security components
- Seats in Use
- Total seats

- Percentage of total licenses in use
- Expiration date
- IP address of license host

Logging Into SmartEndpoint

Note - SmartEndpoint will reach its End of Support (EOS) on December 31, 2025. You can access SmartEndpoint functionality in the Harmony Endpoint Web Management Console. Refer to sk183410.

1. Install an on-premises Endpoint Security Management Server.

   See the *R81.20 Installation and Upgrade Guide* > Chapter *Installing an Endpoint Server* > Section *Installing an Endpoint Security Management Server*.

2. Connect with SmartConsole to the Endpoint Security Management Server.
3. Enable the required Software Blade:
   a. From the left navigation panel, click **Gateways & Servers**.
   b. Open the Endpoint Security Management Server object.
   c. On the **Management** tab, select **Endpoint Policy Management**

      Note -It is not supported to disable **Endpoint Policy Management** on a Security Management Server

   d. Click **OK**.
4. Install the database:
   a. Click **Menu** > **Install database**.
   b. Select all objects.
   c. Click **Install**.
   d. Click **Close**.
5. Open the SmartEndpoint Client:
   a. In the top-left corner of SmartConsole, click **Menu**.
   b. Select SmartEndpoint.

Using SmartEndpoint

Use SmartEndpoint, which connects to the Endpoint Security Management Server, to manage your Endpoint Security environment. This section shows what you can do on each tab in SmartEndpoint.

Note - SmartEndpoint will reach its End of Support (EOS) on December 31, 2025. You can access SmartEndpoint functionality in the Harmony Endpoint Web Management Console. Refer to sk183410.

Overview Tab

The Overview tab shows a graphical summary of important security information about the endpoint clients in your organization. This tab includes three information panes:

Security Summary for the Organization

This pane shows the total number of endpoints discovered in the organization. The pane also shows the number of endpoints that:

- Are aligned with the organizational security policy
- Have security warnings
- Have security violations

Active Alerts

This pane shows the number of active security alerts in different categories. You can click the **View Current Status** link for each category to see the endpoints that generated the alerts. The alert list updates every ten minutes.

You can enable/disable alerts, configure alert thresholds and configure email notifications in **Reporting** tab > **Alerts**. See *"Alerts" on page 67*.

Security Status

This pane shows a chart of different security status categories, including:

- **Deployment Progress** - Shows the progress of package deployment to endpoint computers.
- **Blade Health Check** - Shows which computers have installed components that are not running.

- **Disk Encryption Status** - Shows the status of Full Disk Encryption on endpoint computers.
- **Anti-Malware Updates** - Shows which endpoint computers have or are lacking current Anti-Malware signature updates.
- **Malware Infections** - Shows which endpoint computers are malware-free, have not been scanned, or have malware problems.
- **Compliance Verification** - Shows which endpoint computers are compliant with the security policy and which are restricted or have pending warnings.
- **Bot Detections** - Shows which endpoint computers have bot problems.

For each category you can see:

- **Trend** tab - A line chart that shows the trend over time.
- **Endpoints** tab - A table that shows Endpoint computers in greater detail.

You can also click the **Getting Started** link to run the **Endpoint Security Express Setup Wizard**. Do the steps in the wizard pages to quickly configure the default policy for each component. The wizard also lets you run the *"Active Directory Scanner" on page 124* and configure *"Uploading Client Packages to the Repository" on page 134*.

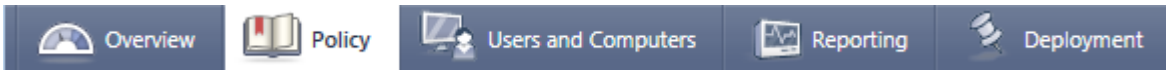
Opening SmartEndpoint

You can open SmartEndpoint in these ways:

- Go to **Start** > **All Programs** > **Check Point SmartConsole <Version>** > **SmartEndpoint <Version>**.
- Open SmartConsole, and from the **Menu**, select **SmartEndpoint**.

Policy Tab

You define and manage the policy for each Endpoint Security component in the Policy tab.



The policy tab contains the **Policy Management Toolbar** and the **Policy Rule Base**.

Users and Computers Tab

The nodes of the Users and Computers tree are filled automatically by an Active Directory scan, or when installed Endpoint Security clients connect to the Endpoint Security Management Server.

The only node whose contents you define and manage is the **Networks** node.

To create a network:

1. Open the **Users and Computers** tab.
2. Right-click **Networks** and select **New Address Range**.

   The **Address Range Properties** window opens.
3. Enter a name for this address range.
4. Enter the first IP address and the last IP address of the range.
5. Add a descriptive comment, and select a color.
6. Click **OK**.

Monitoring Endpoint Security Deployment and Policy

Monitoring your Endpoint Security policy and deployment should be a very important part of your-day-to-day work. The Reporting tab includes many different types of Endpoint Security status reports.

To see monitoring reports:

1. In SmartEndpoint, click the **Reporting** tab.
2. Select a report type from the **Monitoring** tree. The report shows in the pane.
3. Double-click an object in the **User** or **Computer Name** field to open a **Details** window.

   You can assign, create, and change policies from the **Details** window.

Each report shows a summary chart and an **Endpoint List** that shows the users and computers. You can sort and filter the monitoring information by different criteria.

Double-click a user or computer to see its status and the configured rules and actions for each installed component.

Endpoint List Area - Icons and Controls

Item	Description
Search	Enter a text string to search all columns and results that contain the string are shown.
Status:	Select a status to filter by. The options are based on the open report. Endpoints with that status are shown.
In:	Narrow the results to an OU, node or group in the organization. Click to select an item in the **Select Node** window.
	Double click to open the selected user or computer.
	Click to see other options available. Options include *Monitoring Endpoint Security Deployment and Policy*. Some options are not available for all reports. **Add to virtual group** - Add the selected objects to a virtual group. **Toggle chart percentage** - Add and remove the percentages shown on the graph. **Hide Chart/Show Chart** - Close or open the pane with the graph. **Export Report** - Export the report results to an XLS, HTML, or CSV file.

Alerts

The alerts pane shows which endpoint computers are in violation of critical security rules. These violation types can trigger alerts:

- **Certificate Expiration**
- **Compliance Warning**
- **Deployment Failed**
- **Encryption Problem**
- **Anti-Malware Issues**
- High-Availability server out-of-sync:
  - A data batch is in the error state.
  - The synchronization engine is offline.
  - The number of unsent data batches is more than 300. This occurs when the rate at which the synchronization server processes the sync data is lower than rate at which the sync data is generated.
  - A secondary server or a remote help server is not registered as the synchronization engine on the primary server.

The lower section of the pane contains two tabs:

- **Trend** - Shows a line chart showing the trend of security violations over time
- **Endpoints** - Shows the standard endpoint computer list

Configuring Alert Messages

You can configure Endpoint Security to send different types of messages.

Message Type	When Sent	Comments
Initial Alert	Number of endpoints with security violations exceeds the specified threshold	Shows the number of endpoints with violations and the violation type
Alert Reminder	Repeatedly according to a specified frequency as long as the number of endpoints exceeds the threshold	Shows the number of endpoints with violations and the violation type
Alert Resolved	Number of endpoints with security violations falls below the specified threshold	Shows that the alert has been resolved

To define security alerts:

1. On the **Alerts** pane, select a security violation and click **Configure**.

   The **Alert Configuration** window opens.
2. Select how the amount of endpoints that trigger alerts are measured:
   - **Percentage** - The percentage of endpoints in the environment.
   - **Absolute values** - The number of endpoints in the environment.
3. Select a percentage or absolute value for the fields:
   - **Trigger alert when the condition reaches** - When the initial alert message is sent.
   - Optional: **After the alert was triggered, turn off when less than** - When an alert resolved message is sent.
4. In the **Notification Settings** area, select which type of messages to send:
   - Select **Notify on alert activation** to send an Initial Alert message.

     Clear to disable initial alerts.
   - Select **Notify on alert resolution** to send an Alert Resolved message when applicable.

     Clear to disable Alert Resolved messages.
   - Select an Alert Reminder frequency from the **Remind every** list.

     Select **None** (default) to disable reminders.
5. In the **Add New Recipient** field, enter an email address for recipients who will get the alerts.
6. Click **Add**.
7. Click **OK**.

Configuring an Email Server

You must configure your email server settings for the Security Analysis to send alert email messages. If you use Capsule Docs it is also important to configure this. The settings include the network and authentication parameters necessary for access to the email server. You can only define one email server.

To configure the email server:

1. In SmartEndpoint, select **Manage** > **Email Server Settings** > **Configure Settings**.
2. In the **Email Server Settings** window, enter the email server host name or IP address.

3. Select the **Port** number for the email server (default = 25).
4. If the email server requires an SSL connection, select **Enable SSL Encryption**.
5. If email server authentication is necessary, select **User authentication is required** and enter the credentials.
6. Click **Send Test Email** to make sure that you can successfully access the email server.
7. In the window that opens, enter an email address that the test will be sent to and click **Send**.
   - If the verification succeeds, an email is sent to the email address entered and a **Success** message shows in the **Email Server Settings** window.
   - If the verification fails, an **Error** message shows in the **Email Server Settings** window. Correct the parameters errors or resolve network connectivity issues. Stand on the **Error** message to see a description of the issue.
8. Click **OK** to save the email server settings and close the window.

Troubleshooting issues with email settings

If the email server does not send alerts and email server authentication is not necessary do these steps:

1. In SmartEndpoint, select **Manage** > **Email Server Settings** > **Configure Settings**.
2. In the **Email Server Settings** window select **User authentication is required**.

   Configure these parameters :
   - **Port** - Leave the default (25).
   - **User Name** -Enter a fictitious email address. This address will show as the sender of email alerts.
   - **Password** -Enter a fictitious password. This is not used.
3. Optional: Trigger an alert to test the email server.

Performing Push Operations

Push operations are operations that the server pushes directly to client computers with no policy installation required.

Note - If there is no response from the Endpoint Security client, the Push Operation will time out after 24 hours. You must reinitiate the Push Operation.

To add a Push Operation:

1. Go to the **Push Operation** view and click **Add**.
2. Select the push operation and click **Next**.

Category	Push Operations	Windows	macOS	Linux
Anti-Malware	Scan for Malware	Yes	Yes	Yes
	Update Malware Signature Database	Yes	Yes	Yes
	Restore Files from Quarantine	Yes	Yes	Yes
Forensics and Remediation	Analyze by Indicator	Yes	Yes	No
	File Remediation	Yes	Yes	Yes
	Isolate Computer	Yes	Yes	No
	Release Computer	Yes	Yes	No

Category	Push Operations	Windows	macOS	Linux
Agent Settings	Deploy New Endpoints	Yes	No	No
	Collect Client Logs	Yes	Yes	No
	Repair Client	Yes	No	No
	Shutdown Computer	Yes	Yes	No
	Restart Computer	Yes	Yes	No
	Uninstall Client	Yes	Yes	No
	Application Scan	Yes	Yes	No
	Kill Process	Yes	Yes	No
	Remote Command	Yes	Yes	Yes
	Registry Actions	Yes	No	No
	File Actions	Yes	Yes	No
	VPN Site	Yes	Yes	No
	Collect Processes	Yes	No	No
	Run Diagnostics	Yes	Yes	No

3. Select the devices on which you want to perform the push operation.

   Note - You can perform **Run Diagnostics** on only one device at a time.

4. Click **Next**.
5. Configure the operation settings.

Anti-Malware

Push Operations	Description
Scan for Malware	Runs an Anti-Malware scan on the computer or computers, based on the configured settings.
Update Malware Signature Database	Updates malware signatures on the computer or computers, based on the configured settings.
Restore Files from Quarantine	Restores files from quarantine on the computer or computers, based on the configured settings. **To restore files from quarantine:** a. In the **Full Path** field, enter the path to file before it was quarantined including the file name. For example, `c:\temp\eicar.txt` b. Click **OK**.

Forensics and Remediation

Push Operations	Description
Analyze by Indicator	Manually triggers collection of forensics data for an endpoint device that accesses or executes the indicator. The indicator can be a URL, an IP, a path, a file name or an MD5.

Push Operations	Description
File Remediation	Quarantines malicious files and remediates them as necessary. **To move or restore files from quarantine:** a. Click + and select the organization. b. Click **Update Selection**. c. Select the device and click **Next**. d. Add **Comment**, optional comment about the action. e. To move the files to quarantine, select **Move the following files to quarantine**. f. To restore the files from quarantine, select **Restore the following files to quarantine**. g. Click +. h. From the drop-down: i. Select **Full file path or Incident ID**: I. In the **Element** field, enter the incident ID from the Harmony Endpoint Security client or enter the incident UID for the corresponding incident from the Logs menu in the Harmony Endpoint portal. To obtain the incident UID, open the log entry and expand the **More** section to view the incident UID. II. Click **OK** ii. Select **MD5 Hash**: I. Enter or upload the **Element**. II. Click **OK**. i. Click **Finish**.

Push Operations	Description
Isolate Computer	Makes it possible to isolate a specific device that is under malware attack and poses a risk of propagation. This action can be applied on one or more devices. The Firewall component must be installed on the client in order to perform isolation. Only DHCP, DNS and traffic to the management server are allowed.
Release Computer	Removes device from isolation. This action can be applied on one or more devices.

Agent Settings

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Deploy New Endpoints</td><td>Installs the Initial Client on the target devices remotely using any device as the medium to run the push operation. This is suitable if do not have third party tools such as Microsoft System Center Configuration Manager (SCCM) or Intune to install the client.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td>Select the deployment endpoint</td><td>Select the target endpoint or device where you want to install the Initial Client from the organizational tree.
⚠ Caution - The target device must not be the same as the source device.</td></tr>
<tr><td>Endpoint version</td><td>Select the Harmony Endpoint Security Client version to install on the target device.
ⓘ Note - Only Endpoint Security client versions with a corresponding exported package (Manual Deployment of Endpoint Clients) are showed here. You can only push a client version if the package exists in the export packages.</td></tr>
</table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Collect Client Logs</td><td>Collects CPInfo logs from an endpoint based on the configured settings.
For Windows:
For Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory C:\ProgramData\CheckPoint\Endpoint Security\Temp.
For Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory C:\Windows\SysWOW64\config\systemprofile\CPInfo.
For macOS, client logs are stored in the directory /Users/Shared/cplogs.
<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr><tr><td>Log set to collect</td><td>Select the scope of information for the logs.</td></tr><tr><td>Debug Info upload</td><td>Select the location to upload the logs:
Upload CPInfo reports to Check Point servers
Upload CPInfo reports to Corporate server - Update the relevant corporate server information.</td></tr></table></td><td>No</td></tr>
<tr><td>Repair Client</td><td>Repairs the Endpoint Security client installation. This requires a computer restart.
Note - This push operation applies only to Harmony Endpoint Security clients that have been upgraded to a newer version at least once after the installation.</td><td>No</td></tr>
<tr><td>Shutdown Computer</td><td>Shuts down the computer or computers based on the configured settings.</td><td>No</td></tr>
</table>

Push Operations	Description	2FA Required
Restart Computer	Restarts the computer or computers based on the configured settings.	No
Uninstall Client	Uninstalls the Endpoint Security client remotely on the selected devices. This feature is supported for E84.30 client and above.	Yes
Application Scan	Collects all available applications in a certain folder on a set of devices and then adds them to the application repository of the "Application Control" blade on that specific tenant.	No
Kill Process	Remotely kills/ terminate the processes.	No
Remote Command	■ Allows administrators to run both signed (introduced by CP) and unsigned (ones the customer creates) scripts on the Endpoint Client devices. ■ Especially useful in a non-AD environment. ■ Supplies tools/fixes to customers without the need to create new EP client/server versions. ■ Saves passwords securely when provided. The Remote Command feature is supported only in Windows clients running version E85.30 and above	Yes

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Search and Fetch files</td><td>Searches and uploads files to a server.

Supported fields are:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td colspan="2">Search and Fetch files</td></tr>
<tr><td>Locate the following files in the specific folders</td><td>Searches for the files in the specified folders.
a. In the File table, click + .
b. Enter the file name. For example, test.txt or test.zip and click OK.
c. Repeat the steps 1 and 2 for additional files.
d. In the Folder Path table, click +
e. Enter the path and click OK.
f. Repeat the steps 4 and 5 for additional paths.</td></tr>
<tr><td>Locate the following files by exact path</td><td>Searches for the files in the specified path.
a. In the File table, click + .
b. Enter the path where you ant to search for the file and click OK.
c. Repeat the steps for additional paths.</td></tr>
<tr><td colspan="2">Files upload</td></tr>
<tr><td>Select the Upload files to</td><td>Select the checkbox to upload the files to a server.</td></tr>
</table></td><td>Yes</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Corporate Server Info</td><td>a. Specify these:
i. Protocol
ii. Server address
iii. Path on server
iv. Server fingerprint
b. If the server requires login to access it, select the Use specific credentials to upload checkbox, and enter Login and Password.</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Registry Actions</td><td>Add or remove a registry key.

Supported fields:<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td>Action</td><td>Select an action.
Add Key to Registry
Remove Key From Registry
Caution - Removing a registry might impact the endpoint's operating system.</td></tr>
<tr><td colspan="2">Add Key to Registry</td></tr>
<tr><td>Key</td><td>Full path where you want to add the registry key.
For example, Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</td></tr>
<tr><td>Subkey</td><td>Enter the key name to add in the registry. For example, ProductVersion.</td></tr>
<tr><td>Value Type</td><td>Select the registry type.</td></tr>
<tr><td>Value</td><td>Enter the registry value.</td></tr>
<tr><td>Is redirected</td><td>Indicates that virtualization is enabled and add the registry to 32-bit. By default, the registry is added for 64-bit.</td></tr>
<tr><td colspan="2">Remove Key From Registry</td></tr>
</table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Key</td><td>Full path of registry key that you want to delete.
For example, Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis
Caution - Removing a registry might impact the endpoint's operating system.</td></tr>
<tr><td>Subkey</td><td>Enter the key name to remove from the registry. For example, ProductVersion.</td></tr>
<tr><td>Is redirected</td><td>Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.</td></tr>
<tr><td colspan="2">To change the working hours to allow the Anti-Malware signature updates on a DHS compliant Endpoint Security client, see sk180559.</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>File Actions</td><td>Copy, move or delete the file or folder.
Supported fields:
  Note - The folder actions are supported only with the Endpoint Security Client version 87.20 and higher.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td>Action</td><td>Select an action.
■ Copy File
■ Move File
■ Delete File
  Caution - Deleting a file might impact Harmony Endpoint's protected files.</td></tr>
<tr><td colspan="2">Copy File</td></tr>
<tr><td>File path</td><td>Full path of the file or folder you want to copy, including the file or folder name.
Example:
■ For File - C:\Users\<user_name>\Desktop\test.doc
■ For Folder - C:\Users\Username\Desktop\</td></tr>
</table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Target file path</td><td>Full path where you want to paste the file or folder.
Example:
■ For File - C:\Users\<user_name>\Documents
■ For Folder - C:\Users\Username2\
Notes:
■ The file or folder name you specify is used to rename the copied file.
■ If you provide the folder path only, the file is copied with the original file name.
■ If the file or folder already exists, the file is not overwritten and the operation fails.
■ If the file path or target folder does not exist, it is created during the operation.</td></tr>
<tr><td colspan="2">Move File</td></tr>
<tr><td>File path</td><td>Full path of the file or folder you want to move, including the file or folder name.
Example:
■ For File - C:\Users\<user_name>\Desktop\test.doc
■ For Folder - C:\Users\Username>\Desktop\</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Target file path</td><td>Path where you want to move the file or folder.
Example:
■ For File - C:\Users\<user_name>\Documents
■ For Folder - C:\Users\Username1\Documents\
Notes:
■ If you provide the full file path, the is moved with the specified name.
■ If you provide the folder path only, the file is moved with the original file name.
■ If the file or folder already exists, the file or folder is not overwritten and the operation fails.
■ If the file path or target folder does not exist, it is created during the operation.</td></tr>
<tr><td colspan="2">Delete File</td></tr>
<tr><td>File path</td><td>Full path of the file you want to delete, including the file name.
For example, C:\Users\<user_name>\Desktop\test.doc
Caution - Deleting a file might impact Harmony Endpoint's protected files.
Note - Delete folder action is not supported.</td></tr>
</table>
</td><td></td></tr>
</table>

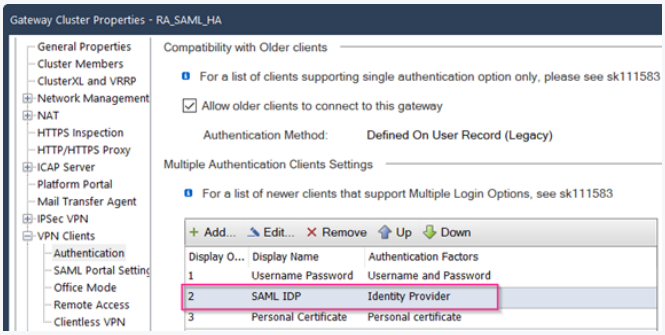
<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>VPN Site</td><td>Adds or removes a VPN site.

Limitations:
■ This is not supported with Linux operating system.
■ You cannot create separate VPN sites for each user that access the endpoint. The same VPN site applies to all users.
■ SoftID and challenge-response authentication methods are not tested.
■ The system does not validate the entries (for example, Server Name or Fingerprint) that you specify.
■ Only one fingerprint operation is supported at a time.
■ You cannot add a new VPN site or remove a VPN site if a VPN site is already connected in the Harmony Endpoint client. Disconnect the VPN site before you add a new VPN site.
■ This operation is not supported if the firewall policy for the client is configured through the on-premise Security Gateway (Policy > Data Protection > Access & Compliance > Firewall > When using Remote Access, enforce Firewall Policy from is Remote Access Desktop Security Policy). To enable the operation on such a client:
a. In the Security Gateway, change the parameter allow_disable_firewall to true in the $FWDIR/conf/trac_client_1.ttm file.
b. Install the policy on the Security Gateway.
c. Reboot the Harmony Endpoint client.
d. Perform the push operation.
Note - If the operation fails with timeout, see sk179798 for troubleshooting instructions.

Supported fields:
<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr></table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Action</td><td>Select an action:
■ Add VPN Site
■ Remove VPN Site</td></tr>
<tr><td colspan="2">Add VPN Site</td></tr>
<tr><td>Server Name</td><td>Enter the IP address or FQDN of the remote access gateway.
Note - Ensure the endpoint can resolve the FQDN to the IP address of the gateway.</td></tr>
<tr><td>Use Custom Display Name</td><td>Select the checkbox if you want to change the display name of the server in the Harmony Endpoint client.</td></tr>
<tr><td>Display Name</td><td>Server name displayed in the Harmony Endpoint client. By default, it uses the Server Name.
To change the display name ,elect the Use Custom Display Name checkbox and enter a display name.</td></tr>
<tr><td>Use Custom Login Option</td><td>Select the checkbox if you want to use a custom login option.</td></tr>
</table>
</td><td></td></tr>
</table>

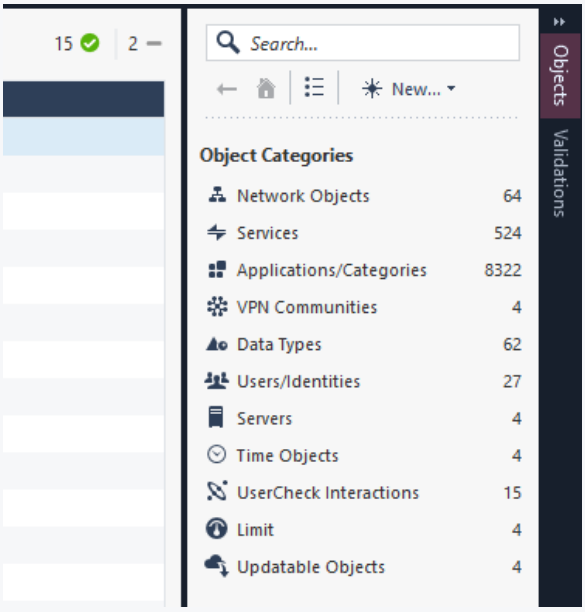
Push Operations	Description	2FA Required

Field	Description
Login Option	Login option for the server. By default, **Standard** login option is selected. To use a custom login option, select **Use Custom Login Option** checkbox, and enter the login option. This must match the Display Name specified in the **GW properties** > **VPN Clients** > **Authentication** > **Multiple Authentication Clients Settings** in the SmartConsole. For example, **SAML IDP**.  For the **Standard** login option, make sure that the **Authentication Method** is **Defined on User Record (Legacy)**. Otherwise, **Standard: does not need authentication method** error appears.

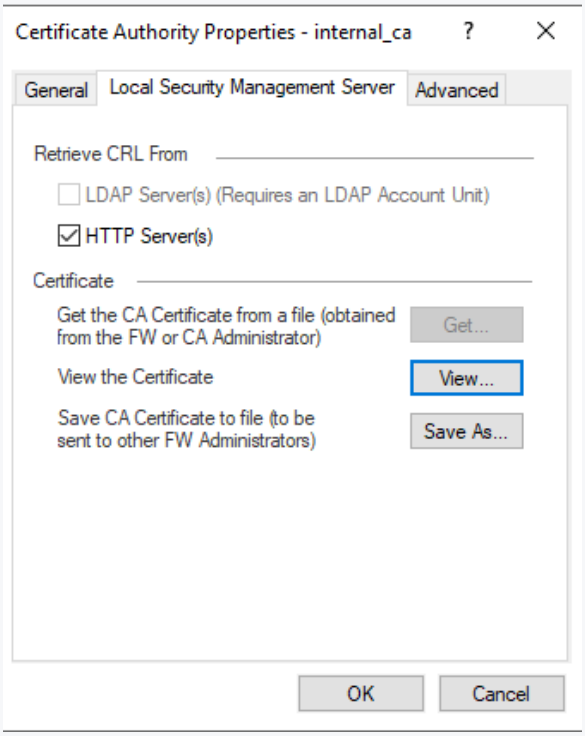
Push Operations	Description	2FA Required

Field	Description
Authentication Method	Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the **Standard** login option: ■ **username-password** ■ **certificate** (for a certificate stored in the CAPI store) ■ **p12-certificate** ■ **securityIDKeyFob** ■ **securityIDPinPad** ■ **SoftID** (not tested) ■ **challenge-response** (not tested) Authentication methods for the custom login option: ■ **Select certificate from hardware or software token (CAPI)** ■ **Use certificate from Public-Key Cryptographic Standard (PKCS #12) file** ■ **Other** **Note** - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select **Other**.

Push Operations	Description	2FA Required

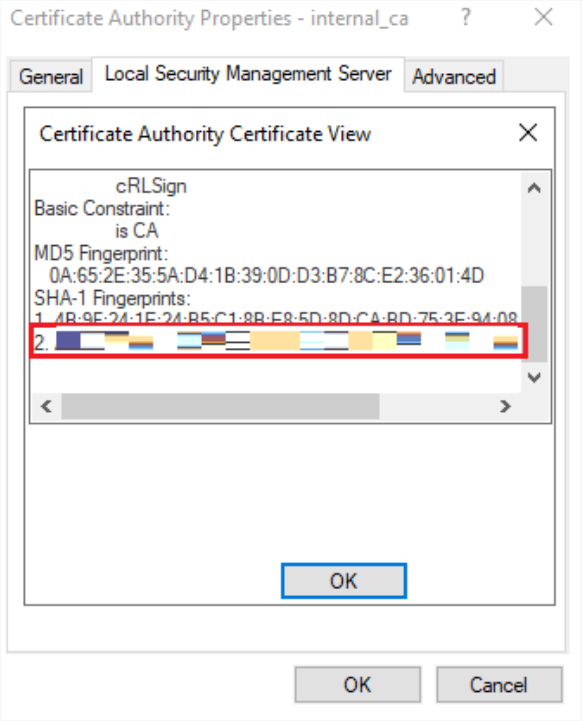
Field	Description
Fingerprint	Enter the fingerprint key. **To get the fingerprint from SmartConsole:** a. In SmartConsole, in the right pane, under **Object Categories**, click **Servers > Trusted CA > internal ca**.  The **Certificate Authority Properties** window appears.

Push Operations	Description	2FA Required

Field	Description
	 b. Click the **Local Security Management** tab. c. Under **Certificate**, click **View**. The **Certificate Authority Certificate View** window appears.

Push Operations	Description	2FA Required

Field	Description



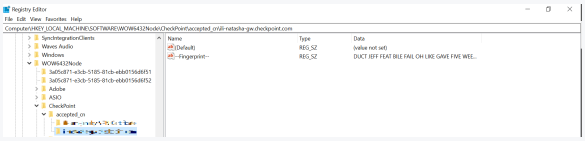
d. Scroll down to **SHA-1 Fingerprints**. The fingerprint is on line number 2.

To get the fingerprint from the device:

a. Manually add the VPN site in the client. For more information, see *Endpoint Security Clients User Guide*.

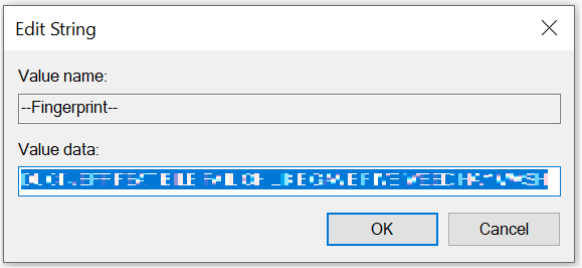
b. After you add and connect to the VPN site successfully, In **Registry Editor**, go to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\accepted_cn*.

c. It displays a folder with the display name of your VPN site.

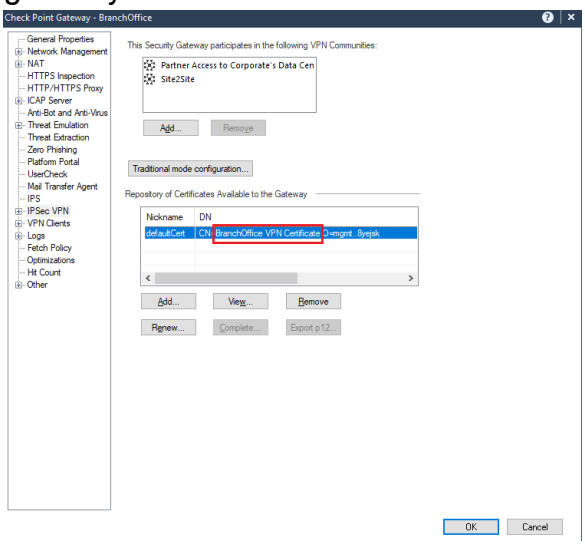


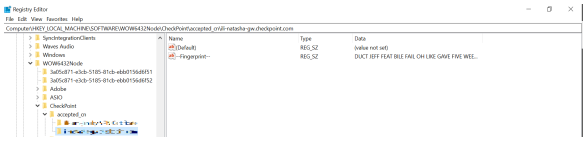
d. Double-click the folder.

Push Operations	Description	2FA Required

Field	Description
	e. In the right pane, under **Name**, double-click **-- Fingerprint--**. The **Edit String** window appears.  f. Copy the fingerprint key from the **Value** data field. g. Click **Cancel** to close the window. h. Paste the fingerprint key in the **Fingerprint** field.

Push Operations	Description	2FA Required

Field	Description
Remote Access Gateway Name	Enter the remote access gateway name. **To get the remote access gateway name from SmartConsole:** a. In SmartConsole, go to **Gateways and Servers**. b. Double-click the gateway. The **Check Point Gateway** window appears. c. Double-click **IPSec VPN**. d. Under **Repository of Certificates Available to the Gateway**, in the table, expand the **DN** column. The value after **CN=** indicates the remote access gateway name.  **To get the remote access gateway name from the device:** a. In **Registry Editor**, go to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\accepted_cn*.

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>b. It shows a folder with the display name of your VPN site. Copy the folder name and paste it in the Remote Access Gateway Name field.
  </td></tr>
<tr><td colspan="2">Remove VPN Site</td></tr>
<tr><td>Display Name</td><td>Enter the display name for the server.</td></tr>
</table>
</td><td></td></tr>
<tr><td>Collect Processes</td><td>Collects information about the process running on the endpoint.

Supported fields:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td>Collect all processes</td><td>Collects information about all the processes running on the endpoint.</td></tr>
<tr><td>Collect process by name</td><td>Collects information about a specific process on the endpoint.</td></tr>
<tr><td>Process name</td><td>Enter the process name. Case-sensitive.</td></tr>
<tr><td>Additional output fields</td><td>Select the additional information you want to view in the collected information.</td></tr>
</table>
</td><td>No</td></tr>
</table>

Push Operations	Description	2FA Required
Run Diagnostics	Runs diagnostics on an endpoint to collect this information: ■ Total CPU and RAM usage in the last 12 hours. ■ CPU usage by processes initiated in the last 12 hours. For example, the CPU used by Anti-Malware to scan files. You can review the CPU usage data to identify processes (scans) that consume CPU more than the specified threshold and exclude such processes from future scans. **Note** - This is supported with Endpoint Security client version E86.80 and higher. **Warning** - Only exclude a process if you are sure that the file is not malicious and is not vulnerable to cyber-attacks.	

6. Under **User Notification**:
   - To notify the user about the push operation, select the **Inform user with notification** checkbox.
   - To allow the user to post pone the push operation, select the **Allow user to postpone operation** checkbox.
7. Under **Scheduling**:
   - To execute the push operation immediately, click **Execute operation immediately**.
   - To schedule the push operation, click **Schedule operation for** and click to select the date.
8. Click **Finish**.
9. View the results of the operations on each endpoint in the **Endpoint List** section (in the **Push Operations** menu) at the bottom part of the screen.

Compliance Status Reports

- **Compliance Status** - Shows endpoint compliance policies that make sure:
  - The correct version of Endpoint Security is installed.
  - The operating system includes all required updates and service packs.
  - Only approved software applications are installed.

  If a user or computer is in violation of a rule, the name of the rule is shown in the **Compliance Violations** column. Names of custom rules are also shown.
- **Top Violations** - Shows the top compliance violations.

These compliance statuses are used in the reports:

- **Compliant** - The computer meets all compliance requirements.
- **About to be restricted** - The computer is not compliant and will be restricted if steps are not done to make it compliant. See *"Configuring the "About to be Restricted" State" on page 392*.
- **Observe** - One or more of the compliance rules that is set as **Observe** is not met. Users do not know about this status and have no restrictions.
- **Restricted** - The computer is not compliant and has restricted access to network resources.
- **Warn** - The computer is not compliant but the user can continue to access network resources. Do the steps necessary to make the computer compliant.
- **Not Running**
- **Status information is missing**
- **Not installed** - The network protection is disabled or not installed.

Activity Reports

The **Activity Reports** group includes these endpoint and Endpoint Policy Server status reports:

- **Endpoint Connectivity** - Shows the last time each endpoint computer connected to the network.
- **Endpoints with Not Running Blades** - Shows the status of components for users and endpoint computers. You can use this report to see which components are running or not running.
- **Protected by Endpoint Security** - Shows if endpoint computers are protected by Endpoint Security.

  You can sort by status:

  - **Unprotected Computers** - Computers that do not have the Endpoint Agent installed.
  - **Unassociated Users** - Users who were identified in the Directory scan but did not log on to a computer with Endpoint Security.
  - **Endpoint Installed** - Computers that have the Endpoint Agent installed.
- **Endpoint Policy Server Status** - Shows Endpoint Policy Server status (Active or Not Active)
- **Endpoint Connectivity by External Policy Server** - Shows which Endpoint Policy Server each endpoint communicates with.

Software Deployment Status Reports

You can select reports that show deployment status by:

- **Deployment Status** - Shows deployment by the status category of deployment.
- **Top Deployment Errors** - Shows the top errors.
- **Deployment by Package** - Shows deployment status by package name
- **Deployment by Policy** - Shows deployment status by profile name

For all Deployment reports, the available status categories are:

- Completed
- Scheduled
- Downloading
- Deploying
- Uninstalling
- Failed Retrying
- Failed

Hold the mouse on an item in the graph to highlight it and see the number of endpoint computers in that status category.

Versions in Use

This group includes these reports:

- **Full Disk Encryption Versions** - Shows the installed version of the Full Disk Encryption component for endpoint clients.
- **Endpoint Package Versions** - Shows the installed version of Endpoint Agent for individual endpoint clients.

Full Disk Encryption Status Reports

There are reports that contain information about the computer encryption and reports that contain information about the Pre-boot.

- **Encryption Status** - Shows the endpoint computer encryption status. The encryption status categories are:
  - Encrypted
  - Decrypting
  - Unencrypted
  - Encrypting
  - System Setup
  - Not Running
  - Status information is missing
  - Not installed
- **Encryption Troubleshooting** - Shows users and computers that might require troubleshooting for disk encryption. You can see the step of the Full Disk Encryption deployment phase that each endpoint computer is in. This information is helpful when it is necessary to find the problem that prevents a computer from becoming encrypted. The status categories are:
  - Initialization
  - Waiting for policy
  - User acquisition
  - Verifying setup
  - Setup protection
  - Deliver recovery file
  - Waiting for restart
  - Encryption in progress
  - Not running
  - Status information is missing
  - Not installed

User Authentication (OneCheck) Status Reports

- **Pre-boot Access Status** - Shows the status of the Full Disk Encryption Pre-boot on each endpoint computer. The status categories are:
  - Pre-boot Enabled
  - Pre-boot Disabled (WIL)
  - Pre-boot Temporarily Disabled (WOL)
  - Not running
  - Status information is missing
  - Not Installed - Full Disk Encryption is not installed on the endpoint.
- **Pre-boot Access Troubleshooting** -Shows users and computers that require troubleshooting for Pre-boot authentication. The issues are divided into two categories: user settings or Smart Card drivers on the computer.
  - **Computers with Smart Card driver issues**. The status can be:
    - No Smart Card users configured, no drivers installed
    - No drivers installed, Smart Card users configured
    - Driver mismatch
  - **Users with password issues or certificate issues**. The status can be:
    - Password not configured
    - Certificate not configured
    - Certificate not valid
    - Certificate does not meet requirements
- **Pre-boot Authentication Methods** - Shows users' configured Pre-boot authentication method and how they last authenticated. You can sort the results by the configured authentication method. The columns in the report are:
  - **Method Used** - The Pre-boot authentication method that the user last used.
  - **Method Configured** - The Pre-boot authentication method configured for the user. This is the configured global **Pre-boot Authentication Settings**, or if overridden, the user's settings.
  - **Method Configured at** - When the configured method was configured.
  - **Last Pre-boot Authentication** - When the user last authenticated to an Endpoint Security client computer.

- **Grace Period Enabled** - If a new authentication method is configured, do users have a period of time that they can still authenticate with the previous method.
- **Grace Period Active** - Is the grace period active at this time for this user.

Media Encryption & Port Protection Status Reports

The main Media Encryption & Port Protection report includes a chart that shows:

- Allowed devices
- Blocked Devices
- Approved by UserCheck (operations)

The **Endpoint List** shows all devices connected to endpoint computers during the last 14 days. It also shows the file operations that were approved by UserCheck justification

- User and computer name
- Status (see above)
- Device name
- Device Category
- Device Serial Number
- Last Event Date
- User Check scenario and reason
- IP Address
- Date of last connection
- Computer type

You can search and filter the list using several criteria.

Discovered Devices

The Discovered Devices report shows all devices that were or are connected to Endpoint Security client computers. If you right-click on a device you can select **Show All Events** to see who used the device, on which computer, and when.

Right-click the header of the **Device Category** column and select **Create Filter** to see only specified devices.

Anti-Malware Status Reports

These reports show the status of Anti-Malware detection and treatment. These reports are available:

- **Anti-Malware Status** - Shows scanning detection statistics
- **Top Infections** - Shows the top ten infections during the past 30 days
- **Anti-Malware Provider Brands** - Shows which endpoints use Check Point Anti-Malware and which use a third-party Anti-Virus provider.
- **Anti-Malware Scanned Date** - Shows status by the last scan date
- **Anti-Malware Updated On** - Shows computers that have Anti-Malware updates installed

Harmony Endpoint Anti-Bot Status Reports

These reports show the status of Anti-Bot detection and prevention. These reports are available:

- **Anti-Bot Status** - Shows detection and prevention statistics
- **Top bots** - Shows the top ten bots during the past 30 days

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:

   ```
   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 OneCheck User Settings, Full Disk Encryption, Media Encryption & Port Protection, and 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 component was installed on the client
  - <Blade> Inherited From - The Active Directory path the rule was originally assigned on and inherited by this machine.

Licenses Report

The **Licenses Status Report** shows the status of the container and component licenses. The summary chart shows the number of seats licensed and the number of seats in use. The licenses list shows detailed license information and status for a selected component or the container. You can export license status information to a file.

To see license warnings, click **Details**.

Deployment Tab

You use this tab to:

- Create Deployment Rules
- Configure Endpoint security client packages for export
- Configure these advanced package settings:
  - VPN client settings
  - The Package repository once uploaded to the server
  - The file signing method to protect the integrity of the client package

Client Logging

Endpoint Security clients upload logs to the Endpoint Security Management Server

On the server, the logs are stored in the common log database, which you can see in the **Logs** tab of the SmartConsole Logs & Monitor view.

Note - The VPN component uploads SCV logs to the VPN Security Gateway.

Client logs are:

- Stored locally at:

  `C:\Documents and Settings\All Users\Application Data\CheckPoint\Endpoint Security\Logs`

Log File	Comments
epslog.1.log epslog.2. log ... ... epslog.<number>.log	• Plain text log file • When the file becomes too large, another is created. • Maximum of 10 log files can exist. When epslog.11.log is created, eplog1.log is deleted. • Can be viewed with any ASCII viewer, or by using the client viewer, or by manually running: `C:\Program Files\Common Files\Check Point\Logviewer\EPS_LogViewer.exe`
epslog.ini epslog.1.elog epslog.1.elog.hmac	Internal files, compressed and encrypted.

- Uploaded according to the Common Client Policy to the Endpoint Security Management Server and viewable in the **Logs** tab of the SmartConsole Logs & Monitor view.
- Client logs can be used for external audit requirements and internal trouble-shooting.

For more details, see the *Endpoint Security Client User Guide for your client release*.

Finding Components

You can use a search feature to find components such as computers, users, directories, and programs.

To find a component:

1. In the **Search** field tool bar, enter a string to match a component.
2. Click **Search**.

   The **Search Results** show on the Users and Computers tab.
3. If the component you are looking for is listed, double-click it.

Alternatively:

Right-click any user shown on the **Reporting** tab and select **Edit**.

Show/Hide components

You can choose which components show in SmartEndpoint and which are hidden.

To show or hide a component in SmartEndpoint:

1. From the **Menu** icon, select **Tools** > **Show/Hide Blades**.
2. Click on a component to see if it is **Visible** or **Hidden**.
3. Click the **Visible** or **Hidden** button to change the setting of the component.
4. Click **OK**.

Users and Computers

You use the Users and Computers tab to see and manage these object types:

- Users
- Computers
- Active Directory OUs and nodes
- Computer and user groups
- Networks
- Virtual Groups

Using the Users and Computers Tab

The Users and Computers tab includes these elements:

- **The Directory Tree** - Shows the Users and Computers hierarchy and structure as folders and objects.
- **Global Actions** - From here you can perform different SmartEndpoint operations.
- **The Blades Pane** - Shows the components and their status for the selected object. Select a component to see its rules and status.
- **The Rule and Status Pane** - Shows the rules and status for the selected component. You can edit rules and do some Full Disk Encryption and Media Encryption & Port Protection actions by clicking items on the toolbar in this pane.

  The Rule and Status pane includes this information for the selected component:

  - The rule name and when it is enforced.
  - Whether the rule is directly assigned to the selected object or inherited from another object.
  - Defined Actions for this rule.
  - Status information for the selected component (if applicable). For OUs and groups, the status section shows selected reports for some components. See *"Monitoring Endpoint Security Deployment and Policy" on page 66*.

Using the Object Details Window

The **Object Details** window shows more detailed information for the selected object than the **Rules and Status** pane. You cannot add or change policy rules in this window.

To show the Object Details window:

1. Go to the applicable object in the **Users and Computers** tree.
2. Right-click the object and select **Edit**. For user and computer objects, you can double-click the object.

The **Object Details** window includes three panes, accessible from a tree on the right side of the window.

General Details - Shows basic information about the selected object and the status of each component. You can click on a component to go to the detailed information pane for that component.

- **Details** (Users and computers only) - Shows LDAP information and groups that the user or computer is a member of.
- **Content** (OUs and groups only) - Shows the members of the selected OU or group.
- components - Shows detailed rule and status information for each component. For OUs and Groups detailed status reports are shown. See *"Monitoring Endpoint Security Deployment and Policy" on page 66*.

Changing Authentication Settings

You can change these OneCheck User Settings in the **User Details** window:

- The *Pre-boot authentication method* when the Full Disk Encryption component is active. The default authentication method is **Password**. See *"Pre-boot Authentication Methods" on page 260*.
- *Lock a user out* after a specified number unsuccessful login attempts from the Pre-boot screen. See *"Account Lock" on page 266*.
- Change a user password.
- Add or remove certificates for smartcard authentication.
- Add or remove authorized computers or groups for Full Disk Encryption Pre-boot.

Using the Users and Computers Tree

The directory tree shows the Users and Computers hierarchy as a set folders and objects. You use the Users and Computers tree to see and select Users and Computers objects.

The tree includes these directories by default:

- **Directories** - Users and computers included in Active Directory OUs.
- **Other Users/Computers** - Users and computers not included in an Active Directory.
- **Networks** - Predefined ranges of IP address.
- **Deleted Users and Computers** - Users and computers that were deleted from the Active Directory.
- **Virtual Groups** - Predefined Endpoint Security groups of users and computers. Members of a Virtual Group can also be part of the Active Directory or a member of other Virtual Groups.

When you right-click an object in the tree, you can do some of these options that show in the option menu, depending on the object type.

- **More Info** - Open the **Object Details** window to see detailed rule and status information. You cannot edit rules or Object Details on this page. You can also use the **More Info** button (in the upper right-hand corner of the pane) to open this window.
- **Using the Users and Computers Tree** - Remove licenses, Full Disk Encryption recovery data, Pre-boot settings, users and logs from the selected computer. See *"Resetting a Computer" on page 120*.
- **Add to Virtual Group** or **Add content to Virtual Group** - Add the object and its members to a virtual group.
- **Add to Favorites** or **Remove from Favorites** - Add or remove the selected object to the **Favorites** list, located under the Users and Computers tree.
- **Full Disk Encryption** - Opens a list of operations related to Full Disk Encryption, Pre-boot, and Remote Help.
- **OneCheck User Settings** - Opens a list of operations related to OneCheck User Settings, Pre-boot, and the *"Check Point Full Disk Encryption Self-Help Portal" on page 237* .
- **Anti-Malware** - Opens a list of Push Operations related to Anti-Malware, Client Settings, and Harmony Endpoint Forensics and Remediation. See *Push Operations*.
- **Harmony Endpoint Forensics and Remediation** - Opens a list of Push Operations related to Harmony Endpoint Forensics and Remediation. See *Push Operations*.

- **Client Settings** - Opens a list of Push Operations related to Client Settings. See *Push Operations*.
- **Address Range** - Define a new address range.

How to use the Users and Computers Tree:

- Use the intelligent **Search Bar** (above the tree) to search for objects. You can use partial words or phrases to see all objects that contain the search text.
- Double-click a parent directory to see its children.
- Click the triangle to go back up to a parent directory.
- Click the Users and Computers toolbar icon to go to the top of the tree.
- Select a user, computer or folder to see its component status and configuration.
- Double-click a user or computer or user to open its **Details** window.

Managing Users

The Users and Computers tab shows status and assigned rules for each component. You can also edit rules and create custom rules as necessary.

To see user details:

1. Select the **Users and Computers** tab.
2. Right-click a user in the **Users and Computers** tree and select **Edit**.

The *"Using the Object Details Window" on page 114* window opens. You can see detailed information as well as rules and status information for each of the components. You cannot change rules and Action settings in this window.

To change rules:

1. Select a user the **Users and Computers** tree.
2. Select a component in the **Blades** pane.
3. Click **Edit Rule**.
4. Do the steps in the **Edit Specific Rule** wizard.

   See the applicable component topics for configuration details.

Managing OUs or Groups

You can manage Active Directory OUs and groups in the Users and Computers tab.

To see OU or group details:

1. Select an OU or group in the **Users and Computers** tree.
2. Right-click an OU or group in the **Users and Computers** tree and select **Edit**.

   The *"Using the Object Details Window" on page 114* window opens. You can see detailed information as well as rules and status information for each of the components. You cannot change rules and Action settings in this window.

To change OU or Group rules:

1. Select an OU or group in the **Users and Computers** tree.
2. Select a component in the **Blades** pane.
3. Click **Edit Rule**.
4. Do the steps in the **Edit Specific Rule** wizard.

   See the applicable component topics for configuration details.
5. On the SmartEndpoint toolbar, select **File > Save**.

Managing Computers

You manage individual computers in the Users and Computers window. This window shows computer details and the policies and user assigned to them. You can configure which users can log on the computer.

To see computer details:

1. Select a computer in the **Users and Computers** tree.
2. Right-click a computer in the **Users and Computers** tree and select **More Info**.

   The **Computer Details** window opens. You can see detailed information as well as rules and status information for each of the components. You cannot change rules and Action settings in this window.

To change rules:

1. Select a computer in the **Users and Computers** tree.
2. Select a component in the **Blades** pane.
3. Click **Edit Rule**.
4. Do the steps in the **Edit Specific Rule** wizard.

   See the applicable component topics for configuration details.
5. On the SmartEndpoint toolbar, select **File > Save**.

Managing Users of a Computer

If the Full Disk Encryption component is included in policy for a specified computer, only users authorized for that computer can log on to it.

Manage the users who can logon to a computer in **Computer Details** > **Security Blades** > **OneCheck User Settings** for a specified computer.

To add authorized users to a computer:

1. Right-click a computer in the Users and Computers tree and select **Full Disk Encryption** > **Authorize Pre-boot users**.
2. In the **Authorized Pre-boot users** window, click **Add**.
3. In the **Select User** window, enter or select a user from the list.

   Add more users as necessary.
4. **Optional**: Select **User Locked** to prevent a user from logging in to any computer.

5. Click **OK**.
6. On the SmartEndpoint toolbar, select **File > Save**.

To remove authorized users from the computer:

1. Right-click a computer in the Users and Computers tree and select **Full Disk Encryption > Authorize Pre-boot users**.
2. In the **Authorized Pre-boot users** window, select a user and click **Remove**.
3. Click **OK**.
4. On the SmartEndpoint toolbar, select **File > Save**.

Resetting a Computer

When the Endpoint Security client is installed on a computer, information about the computer is sent to and stored on the Endpoint Security Management Server. Resetting a computer means deleting all information about it from the server. Resetting a computer does not remove the object from the Users and Computers tree or change its position in the tree.

Important - You can only reset a computer if the Endpoint Security client is not installed. If you reset a computer that has Endpoint Security installed, important data will be deleted and the computer can have problems communicating with the Endpoint Security Management Server.

You might choose to reset a computer if:

- The Endpoint Security Client has been uninstalled or the computer is re-imaged.
- It is necessary to reset the computer's configuration before a new Endpoint Security Client is installed. For example, if the computer is being transferred to different person.

Computer reset:

- Removes all licenses from the computer.
- Deletes Full Disk Encryption Recovery data.
- Deletes the settings of users that can log on to it.
- Removes the computer from Endpoint Security Monitoring.
- Deletes the Pre-boot settings.
- Is marked as unregistered.

After you reset a computer, you must reformat it before it can connect again to the Endpoint Security service.

Note - Resetting a Computer is different than deleting it. If you delete a computer, everything in the databases that is connected to that computer is deleted.

To reset a computer:

1. In the **Users and Computers** tab or anywhere in SmartEndpoint where a computer object is shown, right-click a computer and select **Reset Computer Data**.
2. When the **Reset Computer** message shows, click **Yes** to confirm.
3. On the SmartEndpoint toolbar, select **File > Save**.

Editing Properties of Non-AD Objects

All objects that are not part of an Active Directory are in the **Other Users/Computers** node in the **Users and Computers** tab. From this location you can:

- Edit user and computer properties. You can edit all fields that show a pencil icon.
- Right-click an object and select **Delete** to delete non-AD objects from your environment.

Managing Virtual Groups

In the **Users and Computers** tab you can see and manage Virtual Groups. See *"Virtual Groups in Policy Rules" on page 183*.

Active Directory Scanner

If your organization uses Microsoft Active Directory (AD), you can import users, groups, Organizational units (OUs) and computers from multiple AD domains into the Endpoint Security Management Server. After the objects have been imported, you can assign policies.

When you first log in to SmartEndpoint, the **Users and Computers** tree is empty. To populate the tree with users from the Active Directory, you must configure the Directory Scanner.

The Directory Scanner scans the defined Active Directory and fills the **Directories** node in the **Users and Computers** tab, copying the existing Active Directory structure to the server database.

Required Permissions to Active Directory

For the scan to succeed, the user account related to each Directory Scanner instance requires full read permissions to:

- The Active Directory root.
- All child containers and objects.
- The deleted objects container.

  An object deleted from the Active Directory is not immediately erased but moved to the Deleted Objects container. Comparing objects in the AD with those in the Deleted objects container gives a clear picture of network resources (computers, servers, users, groups) that have changed since the last scan.

The Active Directory Scanner does not scan Groups of type "Distribution".

Required Configuration for Domains

On the Active Directory server, set the Groups Scope to Domain Local only.

Configuring a Directory Scanner Instance

A scanner instance defines which path of the Active Directory will be scanned and the scan frequency. One scanner instance can include the full Active Directory domain, or a part of the domain, for example an OU.

If you want to scan more than one domain or different parts of the same domain, configure in SmartEndpoint more than one scanner. For example, if you want to scan the "HOME" domain and the "OFFICE" domain, configure one scanner instance for each.

Do not create a scanner instance for an OU that is included in a different scan. If you try to create a scan that conflicts with a different scan, an error message shows.

Note - If the scanner is for a specific OU in the domain, only the groups and group members in the OU are included in the scan. If your groups contain members from different OUs we highly recommend configuring the **LDAP Path** of the scan to the root of the domain, to avoid inconsistencies.

If the domains use DNS servers, make sure that:

- The DNS server is configured on the Endpoint Security Management Server.
- The DNS server can supply a list of domain controllers in its domain. We recommend that you configure the DNS server to supply a list of the domain controllers for all domains that the Directory Scanner will scan.

To create a scanner instance:

1. In SmartEndpoint, open the **Deployment** tab > **Organization Scanners**.
2. Click **Add Directory Scanner**.
3. In the **Active Directory Scanner Settings** window:
    - **Domain Name** -Enter the Domain Name in FQDN format, for example, example.com.
    - **Username** and **Password** - Enter the Username and Password of an administrator. The administrator must have read permissions to the scan path and the deleted objects container.
    - **@** -The UPN suffix for the administrator is filled in automatically. Change it if it is different than the FQDN.
4. In the **Advanced** area, select or enter the IP Address of the **Domain Controller**. If the domain has DNS, this is filled in automatically.
5. In **LDAP Path**, click the browse button  to select an OU. If you do not select an OU, the full domain is scanned.
6. You can change the default values in the **Advanced** area:
    - **Connection** - Choose the type of connection for the Directory Scanner communication:
    - **GSS Enabled** - Uses DNS to create Kerberos ticket requests. If DNS is not configured correctly on the Endpoint Security Management Server, the connection is not successful. By default, this is not selected.
    - **SSL Enabled** - Uses SSL Tunneling. You must have an SSL certificate installed on the Domain Controller. By default, this is not selected.
    - **Port** - The port over which the scan occurs.

- **Scan Interval** - The Endpoint Security Management Server sends a request to the Domain Controller to see if changes were made to the domain. If changes were made, the Directory Scanner synchronizes Endpoint Security nodes in the **Users and Computers** tree with nodes in the Active Directory. The Scan Interval is the time, in minutes, between the requests.

7. Click **OK**.

   The scan shows in the **Organization Scanner** window.

Note - Scanning the Active Directory takes time. AD objects show in the sequence they are discovered

The Organization Scanners Page

In the **Deployment** tab > **Organization Scanners** page, you can see all configured scans and their statuses. You can also do these operations:

- **Add Directory Scan** - Configure a scan of an Active Directory domain or OU.
- **Edit** - Edit a configured scan.
- **Remove** - Remove a scan from the list. It will not occur again.
- **Rescan** - Run a selected scan on demand.
- **Start/Stop** - Click the start or stop icon to start or stop a scan.
- **Smart Card certificate scanning setting** > **Configure** - Configure if all user certificates are scanned for Smart Card information during a scanner instance, or only those with the Smart Card Logon OID.

Directory Synchronization

At the specified interval of a scanner instance, the Directory Scanner synchronizes Endpoint Security nodes in the **Users and Computers** tree with nodes in the Active Directory. When synchronization occurs:

- New Active Directory objects are added to Endpoint Security and inherit a policy according to the Endpoint Security policy assignment.
- Deleted users are removed from the **Users and Computers** tree, but only if they had no encrypted removable media devices. Deleted users with encrypted removable media devices move to the **Deleted Users/Computers** folder. The user no longer exists in the Active Directory, but the server keeps the encryption keys for possible recovery.

  You can delete these users manually using SmartEndpoint.
- Computers deleted from the Active Directory that do not have Endpoint Security are deleted from **Users and Computers**.

- Computers deleted from the Active Directory that do have Endpoint Security move to the **Deleted Users/Computers** folder because they might require recovery. You can delete these computers manually from the Management Console.
- Objects updated in the Active Directory are also updated on the server.
- Unchanged records stay unchanged.

Troubleshooting the Directory Scanner

Issue	Solution
The account of the Directory Scanner instance does not have the required read permissions to the Active Directory or to the deleted objects container.	Supply the required permissions.
A corrupted object exists in the Active Directory.	Remove the object or deny the account used by the Directory Scanner read permission to that object. If the corrupt object is a container object, permission is denied for all objects in the container.

SSL Troubleshooting

If you use an SSL connection for the Directory Scanner communication, you might see a message that is related to SSL configuration. Find the problem and solution here.

#	Issue	Solution
1	Stronger authentication is required	Try to connect with SSL with these steps: 1. Get an SSL certificate from your Domain Controller. 2. Import the SSL certificate to the Endpoint Security Management Server. See sk84620. 3. Make sure that SSL Enabled is selected for this Directory Scanner instance.
2	Wrong SSL Port	Change the SSL port or disable SSL. You can do this in the configuration.
3	Cannot connect to the domain controller	Make sure that an LDAP server is running on the LDAP path of the configured domain controller.

#	Issue	Solution
4	SSL certificate is not installed	■ Get an SSL certificate from your Domain Controller and import it to the Endpoint Security Management Server. or ■ Disable SSL.

Configuring DNS for GSS Connections

GSSAPI, Generic Security Service API, is an interface used to access security services. Kerberos is the implementation of GSSAPI used in Microsoft's Windows platform and is supported by Active Directory authentication protocols. During Kerberos authentication, a domain's KDC (Key Distribution Center) must be found through a DNS request.

The DNS server configured on the Endpoint Security Management Server must be able to resolve IP address by name and name by IP address for all domains that are scanned by the Directory Scanner. If DNS is not configured properly, the authentication fails.

Make sure that:

- The DNS server is configured on the Endpoint Security Management Server.
- The DNS server can recognize the DNS servers of all domains that the Directory Scanner will scan.

To make sure the DNS server is configured correctly for GSSAPI authentication:

1. On the Endpoint Security Management Server, run: `nslookup`.
2. Test the name to IP resolving for all domain controllers that are used by the Directory Scanner.
3. Test the IP to name resolving or all domain controllers that are used by the Directory Scanner.

Strengthening Active Directory Authentication to use LDAPS

By default Active Directory authentication uses the LDAP protocol and a simple authentication method. You can make the authentication more secure by changing the authentication protocol to LDAPS, with or without GSSAPI authentication. GSSAPI authentication is based on Kerberos v5.

To change the authentication protocol to LDAPS, GSSAPI, or the two of them:

1. Edit 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`

You can set LDAPS and GSSAPI to true.

3. Save the file.

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 keystores on the Endpoint Security Management Server:

1. 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 a subject that is the FQDN of the Domain Controller. In the example below: `DC.mulberry.com`
   - In which one of certificate extensions has the OID **Server Authentication (1.3.6.1.5.5.7.3.1).**
3. Get the index number of the certificate.

   This is the number which appears in the 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. Download a certificate from the domain controller. Run:

   ```
   certutil -store MY <certificate index> <path_to>\<file name>
   ```

   For example:

   ```
   certutil -store MY 0 C:\certificates\DCCert.cer
   ```

5. Copy the certificate file to the Endpoint Security server. In a High Availability environment, copy the file to the Primary and Secondary servers.

6. Import a certificate to Endpoint Security server keystore. Run:

   ```
   cd $CPDIR/jre_64
   ./bin/keytool -import -keystore ./lib/security/cacerts -file
   <file_name> -alias <alias>
   ```

   For example:

   ```
   ./bin/keytool -import -keystore ./lib/security/cacerts -file
   /home/admin/ServerCert.cer -alias SSLCert
   ```

7. Enter the default password **changeit**.

8. Click **YES** on **Trust this Certificate**.

   A confirmation message **Certificate was added to the keystore** appears.

9. Restart the Endpoint Security servers. Run:

   ```
   uepm_stop
   uepm_start
   ```

Endpoint Security Administrator Roles

Endpoint Security uses the Permissions Profiles configured in SmartConsole to define administrator roles.

Configure Administrators and Permissions in: SmartConsole > **Manage & Settings** tab > **Permissions & Administrators**.

Deploying Endpoint Security Clients

This chapter contains information and procedures for deploying Endpoint Security clients to endpoint computers.

Before deploying the clients, you must add packages to the Repository on the Endpoint Security Management Server. See *"Uploading Client Packages to the Repository" on page 134*

- For clients on Windows, you can use one of these deployment strategies:
  - **Automatic** (recommended) - Use Deployment rules to automatically download and install pre-configured packages on endpoint computers. Define deployment rules and manage deployments using SmartEndpoint. See the status of all deployments in the Reporting tab. See *"Automatic Deployment Using Deployment Rules" on page 139*
  - **Manual** - Export component packages from the Endpoint Security Management Server to endpoint clients using third party deployment software, a shared network path, email or other method. You can only see the deployment status after the package is successfully installed. See *"Manual Deployment Using Packages for Export" on page 145*.
- For clients on Mac, see *"Deploying Mac Clients" on page 151*.

Uploading Client Packages to the Repository

Upload new client versions to the **Package Repository** on the Endpoint Security Management Server.

Endpoint Security Client packages contain the components (also known as *Blades*) to be installed on Endpoint Security clients.

There are a few client packages available for each client release. We recommend that you use the *Dynamic Package*. This is is a self-extracting executable (`*.EXE` file) that contains all components. Other packages are either `EPS.MSI` files for Windows or `zip` files for macOS, that contain different permutations of components.

When you upload packages to the repository on the Endpoint Security Management Server, they are stored by default at `$FWDIR/conf/SMC_Files/uepm/msi`

After you upload a package to the repository, you can choose the components that you want to install on the clients. You can then deploy the packages in one of two ways:

- Automatically, using deployment rules.
- Manually, after exporting the packages.

Endpoint Security Client Packages

These are the client packages. Some may not be available for your client release.

The *Dynamic Package* is a self-extracting executable `EXE` file. All other packages are either `EPS.MSI` files for Windows or `zip` files for macOS.

After you upload the packages to the repository, they are stored by default at `$FWDIR/conf/SMC_Files/uepm/msi`

Directory	Package
`NEWDA`	Initial client This is a very thin client without any components. Used for software deployment.

Directory	Package
`Dynamic`	Complete Endpoint Security Client for any CPU (32-bit or 64-bit). This is a self-extracting executable EXE file with all components (Blades). Only the components you select are part of the exported package, so that it can be much smaller than an exported Windows MSI package. In contrast, MSI packages include all the components in the smallest package in the repository that contains the selected components. You can also configure the Dynamic Package so that it includes only the installation prerequisites that you need, for example .NET or Anti-Malware signatures. Dynamic packages are optimized for upgrades, so the package that is downloaded to the Endpoint Security client includes only the changes from the installed version. This results in a significant decrease in network traffic. A typical download size for an upgrade using the Dynamic Package with all components is less than 200 MB, compared to hundreds of MB for an MSI package. **Best Practice** - Use the Dynamic Package for your client release. Dynamic packages are available for release E82.40 and higher. To use Dynamic Packages for releases E81.40 to E82.30, open a Service Request on the *Check Point Support Center*.
`ATM`	Endpoint Security client for unattended machines, such as ATMs (automated teller machines for bank customers). It runs without a GUI. To learn how to use this package, see sk133174.
`Master_FULL_E1`	Complete Endpoint Security Client for 32-bit systems
`Master_FULL_E1_x64`	Complete Endpoint Security Client for 64-bit systems
`Master_FULL_NO_NP`	Complete Endpoint Security Client without Anti-Malware for 32-bit systems
`Master_FULL_NO_NP_x64`	Complete Endpoint Security Client without Anti-Malware for 64-bit systems
`Master_SBA`	SandBlast Agent Client for 32-bit systems
`Master_SBA_x64`	SandBlast Agent Client for 64-bit systems

Directory	Package
`Master_ENCRYPTION`	Full Disk Encryption and Media Encryption & Port Protection Client for 32-bit systems
`Master_ENCRYPTION_x64`	Full Disk Encryption and Media Encryption & Port Protection Client for 64-bit systems
`Master_TP`	Threat Prevention Client for 32-bit systems: ■ Desktop Firewall and Application Control ■ Anti-Malware ■ Forensics and Anti-Ransomware ■ Anti-Bot ■ Threat Emulation ■ Compliance
`Master_TP_x64`	Threat Prevention Client for 64-bit systems: ■ Desktop Firewall and Application Control ■ Anti-Malware ■ Forensics and Anti-Ransomware ■ Anti-Bot ■ Threat Emulation ■ Compliance

Opening the Package Repository

1. Open SmartEndpoint and connect to the Endpoint Security Management Server.
2. In the **Deployment** tab, click **Software Deployment Rules**.
3. In a Deployment rule, in the **Actions** column, click an **Endpoint Client Version** or **Do Not Install**, and select **Manage Client Versions**.

In the Package Repository, for Dynamic Packages, the **Platform** is *Any CPU*. For other packages the **Platform** is either *64 bit* or *32 bit*.

Uploading a client package to the repository

Important -

- For each release you must choose the type of package you want to use: Either a *Dynamic Package* or an `MSI` package. It is not possible to upload to the repository two types of package for one client release.
- Package deployment fails if you upload both the Dynamic Package and the initial client to the same repository. Upload either one of the files.

1. Open SmartEndpoint and connect to the Endpoint Security Management Server.
2. In the **Deployment** tab, click **Software Deployment Rules**.
3. In a Deployment rule, in the **Actions** column, click an **Endpoint Client Version** or **Do Not Install**, and select **Manage Client Versions**.
4. Select an option:
   - **Load the latest supported client version from the internet** - Download a zip file that contains the most recent packages from the *Check Point Support Center*.
   - **Load a folder containing client installers** - Select a folder that contains packages from your network.
   - **Load client installer file** - Select one package file to upload. The Dynamic Package has the `.exe` extension
   - **Delete package** - Select a package to delete, and click this. Select **Save**. If the package is in use, a message shows that you cannot delete it.

   In the Package Repository, for Dynamic Packages, the **Platform** is *Any CPU*. For other packages the **Platform** is either *64 bit* or *32 bit*.

Configuring a Dynamic Package

After you upload a Dynamic Package to the repository, you can configure the package to further reduce the size of the package that installs on the Endpoint Security clients.

1. Open SmartEndpoint and connect to the Endpoint Security Management Server.
2. In the **Deployment** tab, click **Packages for Export**.
3. Select a Dynamic Package. Those are the packages that have **Additional Settings** in the **Settings** column.
4. In the **Settings** column, select **Additional Settings** and click **Advanced Package Configuration**.
5. In the **Configure Package** window, configure these options:

Page	Option
General	**Disable the Endpoint Security Client's user interface** - For unattended machines, such as ATMs. To learn about packages for ATMs, see sk133174. By default, the client user interface is included in the package.

Page	Option
Dependencies	Select the dependencies to include in the package: ■ **.NET Framework 4.6.1 Installer** (60MB) - Recommended for Windows 7 computers without .NET installed. ■ **32-bit support** (40MB) - Selected by default. Recommended for 32-bit computers. ■ **Visual Studio Tools for Office Runtime 10.0.50903** (40 MB).
Anti-Malware	Choose the signatures to include in the package. This choice determines the level of Anti-Malware protection from the time that a client gets the package until it gets the latest Anti-Malware signatures from the signature provider. ■ **Include Full Signatures** - Recommended for installing on computers without high-speed connectivity to the Anti-Malware server. ■ **Include MIN Signatures** -Selected by default. Recommended for a clean installation on computers that are connected to the Anti-Malware server. ■ **Include NONE signatures** - Recommended for upgrades only.

6. Click **OK**
7. In the SmartEndpoint toolbar, click **Save**.

Automatic Deployment Using Deployment Rules

Use Deployment rules to automatically download and install pre-configured packages on endpoint computers. Define deployment rules and manage deployments using SmartEndpoint. See the status of all deployments in the Reporting tab.

When you deploy Endpoint Security clients with automatic deployment, we recommend that you install two deployment packages on endpoint clients:

1. **Initial Client** -This package includes the Endpoint Agent that communicates with the Endpoint Security Management Server. This must be distributed manually through an exported package.
2. **Endpoint Security Component Package** -This package includes the specified components to be installed on the endpoint client. It can be distributed automatically with Deployment rules.

You can configure the policies for the components before or after you deploy the component package.

Important - You must not change the name of a client MSI package from **EPS.msi**. It is permitted to change the name of a Dynamic Package (the .EXE file).

Getting the Initial Client Packages

The Initial Client is for 32-bit and 64-bit computers.

To get the Initial Client with SmartEndpoint:

1. In SmartEndpoint, open the **Deployment** tab.
2. Under **Initial Client**, click **Download**.

   The **Package download configuration** window opens.
3. Optional: To add users who install this package to a Virtual Group, click the arrow to expand **Virtual Group**.
   - Choose **Select Virtual Group. Endpoints installed with the exported package will automatically be added to it**.
   - Select a Virtual Group or click **Add New** to create a new group.
4. For upgrades from R73: Click the arrow to expand **R73 Client Upgrade**.

a. Select **Support R73 client upgrade**.

b. Optional: To upgrade without user input, select **Silent Upgrade**. If this is not selected, users are prompted to upgrade.

c. Optional: To force reboot after a silent upgrade, select **Force reboot**. If this is not selected, users are asked to reboot.

d. Enter Legacy upgrade passwords if relevant for **Secure Access** and **Full Disk Encryption EW**.

5. Click **Download**.
6. In the Save Location, right-click and select **New** > **Folder**. Give the folder a name that describes the package contents, such as '**Initial Client**.
7. Click **OK**.

   The Endpoint Security Management Server downloads the package from the internet and saves it to the specified folder.

To get the Initial Client from the Support Center:

1. Create a folder for the Initial Client on your local computer.
2. Go the Support Center Web site.
3. Search for Endpoint Security Management Server.
4. In the **Version** filter section, select the latest supported client version.
5. Download **Endpoint Security <version> Client for Windows**.
6. Create a new folder with a name that describes the package contents, such as '**Initial Client**.
7. Copy `EPS.msi` to the folder.

Deploying the Initial Client

You can get the Initial Client from SmartEndpoint, the distribution media, or download an Endpoint Security client from the Support Center. If you do not get the Initial Client from SmartEndpoint, you must give endpoint users the Endpoint Security Management Server host name or IP address. They enter this information to connect to the Endpoint Security Management Server manually.

You can use third-party deployment software to deploy the Initial Client to endpoint computers. The MSI package can be run manually by users or silently by a third party deployment tool.

For new client installations with automatic software deployment, use the **eps.msi** Initial Client.

For upgrades from E80.x and higher, use a complete software package, not the Initial Client.

To upgrade legacy R73 clients, use the **PreUpgrade.exe** Initial Client, which unlocks legacy files using a predefined uninstallation password. It then continues to install the Initial Client package.

Deploying the Endpoint Security Package with Deployment Rules

Deployment rules let you manage Endpoint Security Component Package deployment and updates using SmartEndpoint. The **Default Policy** rule applies to all endpoint clients for which no other rule in the Rule Base applies. You can change the default policy as necessary.

You can define more rules to customize the deployment of components to groups of endpoint computers with different criteria, such as:

- Specified Organizational Units (OUs) and Active Directory nodes
- Specified computers
- Specified Endpoint Security Virtual Groups, such as the predefined Virtual Groups ("All Laptops", "All Desktops", and others.). You can also define your own Virtual Groups.

You must install an Initial Client on endpoint computers before you can deploy components with automatic software deployment.

Creating New Deployment Rules

To create new rules for automatic Deployment:

1. Click the **Deployment** tab and select **Deployment Rules**.
2. Click the **Create Rule icon**.

   The **Create Rule Wizard** opens.
3. In the **Select Entities** window, select an entity (OU, Virtual Group, or Computer). Double-click the node to show the items contained in that node.
4. Click **Next**.
5. In the **Change Rule Action Settings** window,
   a. Click the action.
   b. Select a package version or click **Manage Client Versions** to upload a different client version from in the **Packages Repository**.

c. Select components to install and clear components that are not to be installed with this rule.

6. Click **Next**.
7. In the **Name and Comment** window, enter a unique name for this rule and an optional comment.
8. Click **Finish** to add the rule to the **Deployment Rules**.
9. Click **Save**.
10. Install the policy.

Example Deployment Rules for Virtual Groups

You can deploy Endpoint Security components to Endpoint Security clients according to Virtual Groups.

This example shows Software Deployment Rules that specify the components to be deployed to the *All Laptops* and *All Desktops* Virtual Groups.

Read the comments in the rules.

No	Name	Applies to	Actions	Comment
-	**Software Deployment**			
	Default Deployment	Entire Organization	Do Not install	Default Software Deployment settings for the entire organization
-	**2 more rules**			
1	Deployment to Desktops	All Desktops \Virtual Groups	Endpoint Client Version 80.88.4122 Selected blades	
2	Deployment to laptops	All Laptops \Virtual Groups	Endpoint Client Version 80.88.4122 Selected blades	Same as desktop plus Full Disk Encryption and Endpoint Security VPN

Changing Existing Deployment Rules

To edit rules for automatic Deployment:

1. Click the **Deployment** tab and select **Deployment Rules**.
2. Select a rule.
3. From most columns, right-click to get these options:
   - **Clone Rule** - Make a new rule with the same contents.
   - **Delete Rule** - Delete the rule.
   - **Download Package** - Download the package for export. This includes the Initial Client and Endpoint Security Component Package.
4. To change the name, Double-click the **Name** cell and enter a different name.
5. To change an **Applies To** parameter, right-click an entity and select an option:
   - **Add new entity to this rule** - Select an entity from the tree to add to the rule.
   - **Remove entity from this rule** - Select an entity to delete.
   - **Navigate to item** - Go to the selected entity in the Users and Computers tab.
   - **Add to Virtual Group** - Add the selected entity to a Virtual Group.
6. In the **Actions** column:
   - Select a package version or click **Manage Client Versions** to upload a different client version from in the **Packages Repository**.
   - Select components to install and clear components that are not to be installed with this rule.
7. On the toolbar, click **Save**.
8. Install the policy.

Installing Packages on Clients with Deployment

After the Initial Client is successfully deployed and you have Deployment rules, install Endpoint Security Component Packages from SmartEndpoint.

Edit the Client Settings rules to change client installation settings.

To install Endpoint Security Component Packages on endpoint computers:

1. On the **Deployment** tab, click **Install**.
2. If prompted, click **Save** to save the rules.

3. Select the Rules to install and then click **Install**.

To make sure that a rule does not install:

Right-click in the Actions column of a Deployment rule and select **Do not install**.

Manual Deployment Using Packages for Export

You can export a package of Endpoint Security components from the Endpoint Security Management Server to endpoint clients using third party deployment software, a shared network path, email or other method.

When you create package of Endpoint Security components for export, the Initial Client is usually included in the package, and not installed first.

You can only see the deployment status after the package is successfully installed.

The procedure for creating a package is almost the same as for defining a Deployment Rule. You select different sets of components for Desktop computers and laptops in a package. The package installation program automatically detects the computer type and installs the applicable components.

Creating or Changing a Package for Export

1. In the **Deployment** tab, select **Packages for Export**.
2. To add a new package, click **Add Package**.

   The new package shows at the bottom of the list.
3. Double-click the **Name** cell in the applicable package and enter a package name.
4. **Optional**: Double-click the **Version** cell and select a different Endpoint Client version from the list.

   You can select **Manage Client Versions**, to add more package versions to the repository.
5. Click the **Desktop Blades** and **Laptop Blades** cells and then select the components to include in each package.
6. Optional: In the **Settings** column select a **Virtual Group** or create a new one. Users who install this package will automatically be put in this Virtual Group.
7. Optional: In the **Settings** column, if you defined an **Endpoint Connect VPN** component, right-click the VPN setting and do one of these actions:
   - Select a predefined VPN site from the list.
   - Use a local VPN settings file
   - Add a new VPN site
8. If you are upgrading legacy Endpoint Security release, in the **Settings** column:

- Double-click the legacy upgrade option and select **Support client pre-install upgrade**.
- Select **Silent mode active** or **Silent mode not active**.
- Select the **Legacy Secure Access** option and click **Configure Upgrade Password** to enter and confirm the password.
- Select the **Legacy Full Disk Encryption EW** option and click **Configure Upgrade Password** to enter and confirm the applicable passwords.

9. In the **Software Deployment Rules** window, click **Save**.

Deleting a Package Definition

To delete an existing package definition, select the package **Name** and click **Remove Package**.

Defining a VPN Site

When you use an exported package, you can configure each component package to connect to a default VPN site.

You can configure a default VPN site for packages for export. You cannot configure a default VPN site with automatic Deployment rules. To distribute a defined VPN site with Deployment rules, you can:

- Use Deployment rules to distribute an Endpoint Security component package without **Endpoint Connect VPN**.
- Create a package for export that includes only **Endpoint Connect VPN** and distribute it manually.

By default, no VPN site is defined for a new package. In the **Packages for Export** window, in the **Settings** cell of the package, the default setting is **No VPN site defined**.

To configure a client package with a default VPN site:

1. In the **Deployment** tab, go to the **Packages for Export** page and select a package. Make sure it includes **Endpoint Connect VPN** in the**Selected blades**.
2. In the **Deployment** tab, go to **Advanced Package Settings** > **VPN Client Settings**.
3. Click **New**.
4. In the **Endpoint Secure Configuration** window, enter the VPN Site details:
   - **Display Name** - Unique name for this VPN site
   - **Site address** - Site IP address
5. Select an **Authentication Method** from the list:

- **Username-password** - Endpoint users authenticate using their VPN user name and password
- **CAPI certificate** - Endpoint users authenticate using the applicable certificate
- **P12 certificate** - Endpoint users authenticate using the applicable certificate
- **SecurID KeyFob** - Endpoint users authenticate using a KeyFob hard token
- **SecurID PinPad** - Endpoint users authenticate using the an SDTID token file and PIN
- **Challenge-response** - Endpoint users authenticate using an administrator supplied response string in response to the challenge prompt.

6. Click **OK**.

Exporting a Package

1. In the **Packages for Export** window, select a package.
2. When using a Dynamic Package, configure the exported package.In the **Settings** column, select **Additional Settings** and click **Advanced Package Configuration**. See *"Configuring a Dynamic Package" on page 137*
3. Click **Download Package**.
4. In the **Export Package** window:
   a. For dynamic packages, **Any CPU** is selected.For MSI packages, select the platforms (**32-Bit** and/or **64 bit**) to export for laptops and desktops.
   b. Click **Download**.
5. Click **OK**.
6. Select a location to save the files.

   The package are downloaded to the specified path. A different folder is automatically created for each option selected in step 3a. When using Dynamic Package, the name of the exported package is `EPS.exe`. Otherwise, the name of the package is `EPS.msi` and/or `PreUpgrade.exe`.

Installing an Exported Package on a Client Computer

Send the package to the users. When using Dynamic Package, the exported package is a self extracting executable (`*.EXE`). By default, the filename is `EPS.exe`. For other types of package, the name of the package is `EPS.msi` and/or `PreUpgrade.exe`.

Endpoint users manually install the packages. On Windows 8.1 and higher clients, you must install an exported package with **Run as administrator** selected. You cannot install it with a double-click.

You can also use third party deployment software, a shared network path, email, or some other method

Configuring Software Signatures for Packages for Export

You can select a file signing method for MSI files that will be deployed using an external distribution system.

The Endpoint Security Management Server keeps the certificate in the specified folder.

By default, the client uses an internal signature to authenticate.

To create a custom signature:

1. Open the **Deployment** tab > **Advanced Package Settings > Software Signature** page.
2. In the **Certificate Settings** area select one of these file signing methods:
   - None
   - Internal
   - Custom

   If you select custom, do these steps:
   a. Click **Browse** and get the certificate (*.p12 file).
   b. Enter a name and password for the certificate.

      The certificate is created on the Endpoint Security Management Server.
   c. Send the *.p12 file to client computers before you install the client package.

Seeing the Deployment Status

To see the component deployment status:

1. Go to the **Reporting** tab.
2. Select **Deployment** from the tree.
3. Select one of the Deployment status reports.

Deploying Mac Clients

You can distribute the client packages for Mac clients manually or automatically.

Getting the Mac Client

To get the Mac client package:

1. In the **Deployment** tab, under **Mac Client**, click **Download**.
2. In the window that opens, select which components to include in the package and click **Download**.

   If more than one version is in the Package repository, select a client to download.
3. **Optional**: If **Remote Access VPN** is part of the package, you can configure a VPN site.
4. Select the location to save the package.

   The package starts to download.
5. The package, **Endpoint_Security_Installer.zip** shows in the configured location. This is the file that you distribute to endpoint users.

Manual Deployment

To distribute the Mac client package:

Use a third party distribution method to distribute the **Endpoint_Security_Installer.zip** file to endpoint users.

To install the Mac client package on client computers:

1. Double-click the **ZIP** file to expand it.
2. Click the **APP** file that shows next to the zip file.

   The Check Point Endpoint Security Installer opens.
3. Click **Install**.
4. Enter a **Name** and **Password** to authorize the installation.
5. Click **OK**.

   Wait while package installs.
6. A message shows that the package installed successfully or failed for a specified reason.

Click **Close**.

If the installation was successful, the Endpoint Security icon shows in the menu bar.

Automatic Deployment Using Tiny Agent

Tiny Agent is small executable file (less than 2 MB) that automatically downloads and installs the Initial Client.

It is available for:

- Cloud-deployments with Endpoint Security Management Server R81.10 Take 45 or R81.00 Take 123 or higher.
- On-premise deployments with Endpoint Security Management Server R81.20 or higher.

To download the Tiny Agent:

1. Click **Overview** > **Download Endpoint** (on the top banner).
2. Click **Policy** > **Deployment Policy** > **Software Deployment**, and click **Download Endpoint** (on the top banner).

   The system downloads the **EPS_TINY.zip** file.
3. Unzip the **EPS_TINY.zip** file and run the application.

Uninstalling the Client

To uninstall the Endpoint Security client on Mac computers:

1. Open a terminal window.
2. Run:

   ```
   sudo "/Library/Application Support/Checkpoint/Endpoint Security/uninstall.sh"
   ```

   If the Endpoint Security client was encrypted, the uninstall script first prompts for a reboot so that the volumes can be decrypted. After decryption, the script continues to uninstall the client.

   After you uninstall the Endpoint Security client, the administrator must reset the computer through SmartEndpoint on the Security Management Server. See *"Resetting a Computer" on page 120*.

Upgrading Endpoint Security Clients

This section includes procedure for upgrading endpoint clients:

You can upgrade to E8X.x clients from earlier versions of E8X.x clients with these requirements:

- You must upgrade both the Initial Client and the Endpoint Security Component Package at the same time. You cannot upgrade the Initial Client by itself.
- During the upgrade you cannot remove the Full Disk Encryption component.
- You can change all other components and all component configuration settings.

Client upgrade workflow:

1. Make sure that the clients are connected to an Endpoint Security Management Server of the higher version.
2. Get a complete package with Initial Client and the Endpoint Security Component Package. Get this from the **Deployment** tab in one of these ways:
   - **Download** a package from the **Packages for Export** window.
   - In the **Software Deployment Rules** window, right-click in a rule and select **Download Package**. This includes the Initial Client and Endpoint Security component package.
3. Deploy the package.

Upgrading with Deployment Rules

The Client Settings Policy controls if users can postpone an upgrade installation or if the upgrade is installed on clients immediately. You can configure the settings in the **Client Settings** Policy. Edit the **Default installation and upgrade settings**.

To upgrade clients with Deployment Assignments:

1. In the **Deployment** tab, select a rule and change its **Endpoint Client Version** in the **Client Version** column.

   All computers are assigned to that Policy rule will be upgraded.
2. Optional: Change who the rule applies to in the **Applies To** column.
3. Select **File** > **Save** or click the **Save** icon.
4. Select **File** > **Install Policies** or click the **Install Policies** icon.

5. The Endpoint Agent on each assigned client downloads the new package. The client installation starts based on the settings in the Client Settings policy rule. You can configure:
   - If the Client Settings policy forces installation and automatically restarts without user notification.
   - If the Endpoint Agent sends a message to the user that an installation is ready and gives the user a chance to postpone the installation or save work and install immediately.
6. The Endpoint Agent installs the new client.

   If the user does not click **Install now**, installation starts automatically after a timeout.
7. After installation, the Endpoint Agent may reboot the computer.

Upgrading with an Exported Package

Upgrade a client to a new package that includes the same components as it has now. Add and remove components after the upgraded package is installed.

To upgrade clients with an exported package:

1. In the **Deployment** tab, go to **Packages for Export**.
2. select a package and click **Upgrade Profile**.

   A message opens that shows if an update is available.
3. Click **Yes** to confirm that you want to upgrade the profile.
4. In the **Export Package** window:
   a. For dynamic packages, **Any CPU** is selected. For MSI packages, select the platforms (**32-Bit** and/or **64 bit**) to export for laptops and desktops.
   b. Enter or browse to a destination folder.
5. Click **OK**.

   The package files are downloaded to the specified path. A different folder is automatically created for each option selected in step 4a. When using Dynamic Package, the exported package is a self extracting executable (`*.EXE`). By default, the filename is `EPS.exe`. For other types of package, the name of the package is `EPS.msi` and/or `PreUpgrade.exe`..
6. Send the package files to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.

   You can also use third party deployment software, a shared network path, email, or some other method.

Gradual Upgrade

To upgrade more gradually, you can create a new deployment profile and distribute it only to specified computers.

Note - For an exported package, save the new package in a different location than the previous package

When you are prepared to upgrade all clients, upgrade all deployment profiles.

Upgrading Legacy Clients

To see the supported upgrade paths, see the *Release Notes for the Endpoint Security client version, to which you want to upgrade*. Legacy clients are those earlier than version E80. You must enter password information to upgrade legacy Secure Access and Full Disk Encryption.

Offline Upgrades

During an offline upgrade, the endpoint has no connection with the Endpoint Security Management Server. For this reason, the `Preupgrade.exe` package delivered to the client must contain:

- All the passwords necessary to successfully uninstall legacy products
- The new client with the necessary components and policies

Offline upgrades use the `Preupgrade.exe` file, which is automatically created in the same directory as the MSI package.

To create an offline upgrade package:

1. On the **Deployment** tab, select **Packages for Export** from the tree.
2. Click **Add**.

   A new package shows in the list.
3. Optional: Change the package **Name** and **Version**.
4. In the **Settings** column, select **Support client preinstall upgrade**.
5. Under **Support client preinstall upgrade**, make these selections as necessary:
   a. **Silent Mode** - Choose if silent mode is active. When active, the procedure tool runs silently without user intervention. If silent mode is not active, users can see the GUI of the Upgrade tool. If silent mode is active, select what happens after the upgrade:
      - **Force restart after upgrade**.
      - **Prompt user to restart after upgrade**.
   b. **Secure Access upgrade** - To enable a Secure Access upgrade you must enter the uninstallation password. Click on **Legacy Secure Access upgrade not supported** and select **Configure Upgrade Password**.

      In the **Legacy Secure Access Upgrade** window, select **Support Legacy upgrade** and enter and confirm the uninstallation password.

c. **Legacy Full Disk Encryption upgrade** - To enable an upgrade from legacy Full Disk Encryption EW, you must enter the uninstallation password. Click on Legacy Full Disk Encryption EW upgrade not supported and select **Configure Upgrade Password**.

   In the **Legacy Full Disk Encryption EW** window, select **Support Legacy upgrade** and enter and confirm the uninstallation password.

6. Make sure the components in the **Desktop Blades** and **Laptop Blades** columns are correct.
7. Optional: In the **Settings** column, add a Virtual Group destination for the package. Click **Do not export to Virtual Group** and select **New**.
8. Select **File** > **Save**.
9. Select the package and click **Export Package**.
10. In the **Export Package** window:
    a. Select the platform versions (32/64 bit) to export for laptops and desktops.
    b. Enter or browse to a destination folder.
11. Click **OK**.

    The **PreUpgrade.exe** files are downloaded to the specified path.
12. Send the **PreUpgrade.exe** files to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.

    You can also use third party deployment software, a shared network path, email, or some other method.

To install the offline upgrade, users must:

1. Double-click `Preupgrade.exe`.
2. Follow the on-screen instructions to install the package.

Online Upgrades

During an online upgrade the endpoint has a connection to the server. When the initial client is installed, it connects to the server. The initial client uses the **Common Client Settings** that contains uninstall passwords for legacy products.

To create a package for an Online upgrade:

1. In the **Policy** tab > **Client Settings** section, and right-click **Default installation and upgrade settings**.
2. Click **Edit Properties**.

The **Installation** window opens.

3. Click **Legacy Client Uninstall Password**.
4. Enter uninstall passwords for:
   - Legacy Secure Access
   - Legacy FDE EW
5. Click **OK**.
6. On the **Deployment** tab, select **Packages for Export** from the tree.
7. Click **Add**.
8. Add a package with **Initial Client Only**, with the version you require.
9. Click **Export Package**.
10. In the **Export Package** window:
    a. Select the platform versions (**32 bit**, **64 bit**, or **Any CPU**) to export for laptops and desktops.
    b. Enter or browse to a destination folder.
11. Click **OK**.

    The package **EPS.msi** files (or **EPS.exe** for Dynamic Package files) are downloaded to the specified path.
12. Send the exported package to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.

    You can also use third party deployment software, a shared network path, email, or some other method.

After the package is installed, you can add a package with Endpoint Security components. See *"Upgrading with Deployment Rules" on page 153*.

Upgrading Legacy Full Disk Encryption

To see the supported upgrade paths, see the *Release Notes for the Endpoint Security client version, to which you want to upgrade*.

Before you upgrade, make sure that encryption or decryption are not running.

You do the upgrade using the standard Endpoint Security MSI packages, which can be run manually or through Endpoint Security software deployment.

During the upgrade:

- The client remains encrypted.
- All existing user and policy settings are discarded. Only partition keys are kept.
- Full Disk Encryption goes through the Deployment Phase

To upgrade a client package from Full Disk Encryption EW:

- If you know the Validation Password, do the procedure in *"Upgrading Endpoint Security Clients" on page 153*.
- If you do not know the Validation Password, do the procedure below.

To upgrade a client package from Full Disk Encryption MI or from EW without the password:

1. In the existing MI or EW environment, create a user or user group with this name:

   `_allow_upgrade_`

   This user or group does not require permissions.
2. Update all of the Full Disk Encryption MI or EW clients with the new user or group.
   a. In the Full Disk Encryption MI or EW Management Console, go to the container that contains all clients.
   b. Right-click the object and select **Properties**.
   c. In **Properties** > **Software** tab, select **Full Disk Encryption** and click **Properties**.
   d. Expand **User Group**, right-click **Users**, and select **Add Users**.
   e. Browse to find the `_allow_upgrade_` user and select **Add to Selected Users**.
   f. Click **OK**.
3. Make sure that all clients are connected to the server and receive the update after the next heartbeat.
4. Install a new Initial Client on the legacy client computers.

To upgrade a client package from Full Disk Encryption for Mac:

Do the procedure in *"Upgrading Endpoint Security Clients" on page 153*.

What effect does an upgrade have on users?

- Users are instructed to use their Windows password for the first Pre-boot after the upgrade and deployment completes.
- The Pre-boot page looks slightly different.

Do not:

- Upgrade when the disk is not fully encrypted.
- Start another upgrade before a computer is fully protected with the first upgrade.
- Uninstall the upgrade before a computer is fully protected with the upgraded version.

Troubleshooting the Installation

Administrative Privileges

Installation of Endpoint Security requires the user to have administrator privileges.

- Installing or uninstalling the client on Windows 7 and higher with active UAC (User Access Control) requires the user to invoke the installer with the "run as administrator" option.

  To enable this right-click mouse option, add the following information to the registry:

  ```
  [HKEY_CLASSES_ROOT\Msi.Package\shell\runas\command]
  @=hex
  (2):22,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,
  00,6f,00,74,\
  00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,0
  0,5c,00,6d,00,\
  73,00,69,00,65,00,78,00,65,00,63,00,2e,00,65,00,78,00,65,00,2
  2,00,20,00,2f,\
  00,69,00,20,00,22,00,25,00,31,00,22,00,20,00,25,00,2a,00,00,00
  ```

- To install or uninstall using the command line, the user must have administrator privileges ("Run as administrator").
- Microsoft packages. During installation, the 1720 error message may occur:

  ```
  "Error 1720. There is a problem with this Windows Installer
  package.
  A script required for this install to complete could not be
  run.
  Contact your support personnel or package vendor.
  Custom action ExtractConfigs script error -2147024770, : Line
  2, C?"
  ```

  Microsoft suggests **KB311269**: Register the `WScript` object by running the "`wscript -regserver`" command from a command prompt or from the **Run** option on the Start menu.

- For information about the DES encryption on Windows 7 clients, see *"Step 1 of 3: Configuring the Active Directory Server for Authentication" on page 209*.

Repairing Clients

If a client deployment fails, you can Repair the client, which installs the Endpoint Security client on the computer again. Repair a client in one of these ways

- Run **Repair** from *Push Operations* in SmartEndpoint.
- Run Repair from the endpoint computer. Administrator privileges are required.

To repair an Endpoint Security client from the endpoint computer on Windows:

1. Make sure that the original **EPS.msi** and **PreUpgrade.exe** files are on the endpoint computer.
2. Go to **Control Panel** > **Programs and Features** > **Uninstall or change a program**.
3. Right-click **Check Point Endpoint Security** and select **Repair**.

EPS Service for VPN Connectivity

If the VPN client is unable to connect to the configured Security Gateway, a **Connectivity to the VPN server is lost** message shows. To resolve this:

1. Make sure that the **Check Point Endpoint Security** service (the EPS service) is up and running.
2. If this service does not exist, install it by opening a command prompt and running:

```
"c:\Program Files\CheckPoint\Endpoint Security\Endpoint
Connect\TracSrvWrapper.exe" -install
```

Uninstalling the Client on Windows

Administrator privileges are required to uninstall the client.

To uninstall the Endpoint Security client on Windows computers:

1. Make sure that the original `EPS.msi` and `PreUpgrade.exe` files are present on the endpoint computer.
2. Go to **Control Panel > Programs and Features > Uninstall or change a program**.
3. Uninstall the Endpoint Security client.
4. If the client has Full Disk Encryption installed, run the **Uninstall or change a program** applet again after the disk completes the decryption.

After you uninstall the Endpoint Security client, you must reset the computer through SmartEndpoint on the Security Management Server. See *"Resetting a Computer" on page 120*.

Note - We recommend that you run a database backup on a daily basis.

Configuring Logging

Each Endpoint Security client sends logs to the Endpoint Security Server (Endpoint Policy Server or Endpoint Security Management Server) to which the client is connected.

To see all collected logs together in the **Logs** tab of the SmartConsole Logs & Monitor view, you must configure Log Indexing for each Endpoint Security Server in the SmartConsole.

Do this procedure for each Endpoint Security Server.

To configure Logging from one Endpoint Security Server to a different Endpoint Security Server:

1. Open SmartConsole and connect to the Endpoint Security Management Server.
2. Open the Endpoint Security Management Server object.
3. In the tree of the window that opens, select **Logs** > **Log Server**.
4. Select **Enable Log Indexing**.
5. Click **OK**.
6. Select **Menu** > **Install Database** and install the database on all hosts.
7. Run `cprestart` on the Endpoint Security Management Server.

Backup and Restore

Endpoint Security lets you back up all security data, such as users and policy information, to one compressed file. Using a command line migration utility, the backed-up data can be restored to an off-line Endpoint Security Management Server.

If you have High Availability, this is usually not necessary.

The compressed package contains:

- Configuration files
- Client packages
- Certificates for client packages
- Endpoint Management database
- Security Management Server database

The migration utility:

- Only exports and imports files that are related to Check Point components installed on the target server.
- Copies configuration files to the correct path.smartda

Prerequisites

- The two Endpoint Security servers must have the same Endpoint Security version.
- The two Endpoint Security servers must have the same Check Point products installed.
- The offline target server must have the same IP address and hostname as the source server.
- The source and the target servers are primary Endpoint Security servers. The export and import operations are not supported from or to a secondary server.

How to Back Up and Restore

Use the `migrate` utility to back up and restore Endpoint Security files.

See *Backing Up and Restoring* in the *R81.20 Installation and Upgrade Guide* .

Updating the PAT Version on the Server after Restore

Restoring an earlier configuration (.tgz) file to a new Endpoint Security Management Server also restores the older Policy Assignment Table (PAT). If the PAT version on the restored server is lower than the PAT version on the client, the client will not download policy updates.

If you made a backup the database of your Endpoint Security Management Server, and later restored it, then you must follow these steps:

To get the PAT version from a client connected to the server:

1. Open the Windows registry.
2. Find `HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\EndPoint Security\Device Agent`
3. Double-click the **PATVersion** value.

   The **Edit String** window opens.
4. Copy the number in the **Value data** field. This is the PAT version number.

To change the PAT version on the server:

1. Open a command prompt.
2. Change directory to:

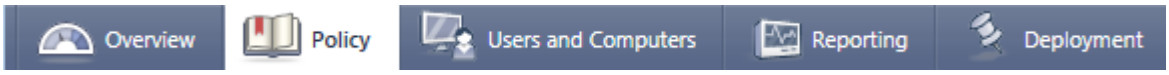
   ```
   $UEPMDIR/bin
   ```
3. Run the Endpoint Security Management Security utility and set the new PAT version:

   ```
   uepm patver set <old_PAT_version_number> + 10
   ```
4. Make sure the new PAT version is set by running:

   ```
   uepm patver get
   ```

Defining Endpoint Security Policies

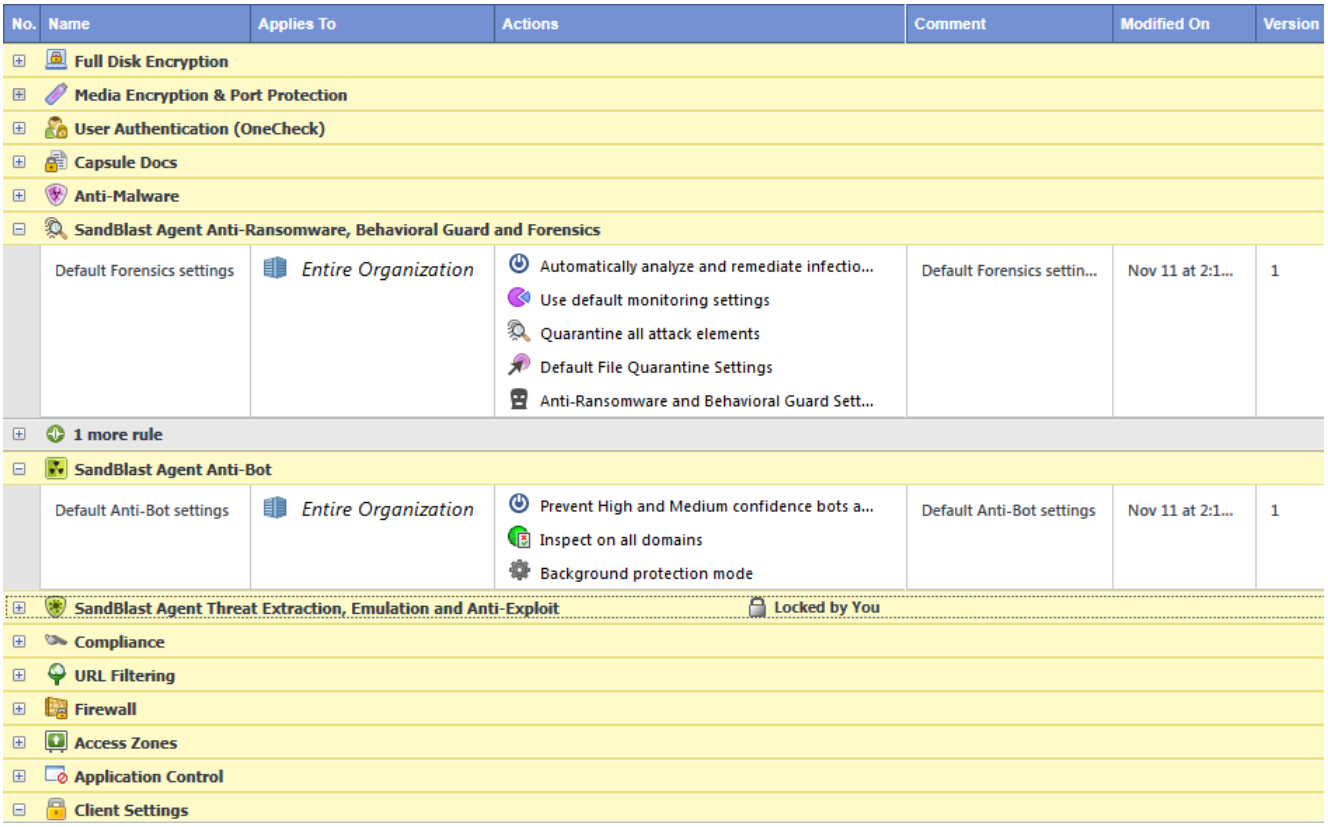
To manage the Security Policies for Endpoint Security, use the **Policy** tab of the SmartEndpoint console.



The **Policy** tab contains the **Policy Management Toolbar** and the **Policy Rule Base**.

The **Policy Rule Base** contains a policy for each of the Endpoint Security components (formerly known as a *Blades)*. These policies enforce protections on endpoint computers.

The policy for each component is made up of rules. This shows some example of rules in the **Policy** tab:



Each rule applies to a specific component, and to a specific part of the organization. Each rule has a set of actions.

The policy for each component has a *default rule* that applies to the *entire organization*. You can change the actions of a default rule, but you cannot make the default rule apply to a specific part of the organization. You cannot delete the default rule.

You can create new rules that apply to specific parts of the organization.

Columns of a Policy Rule Base

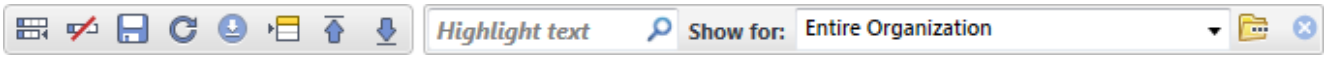
These are the columns in a policy rule:

Column	Description
No.	Rule Number
Name	Rule Name
Applies To	The part of the organization (the *entity*) to which the rule applies
Actions	The configurations that apply to the Endpoint Security component
Comment Modified On Version	Informational fields. Right-click a column to select the fields to show. You can also show: ■ Created On ■ Deployed In ■ Modified By

The Policy Toolbar

The **Policy** tab contains the **Policy Toolbar** and the **Policy Rule Base**.

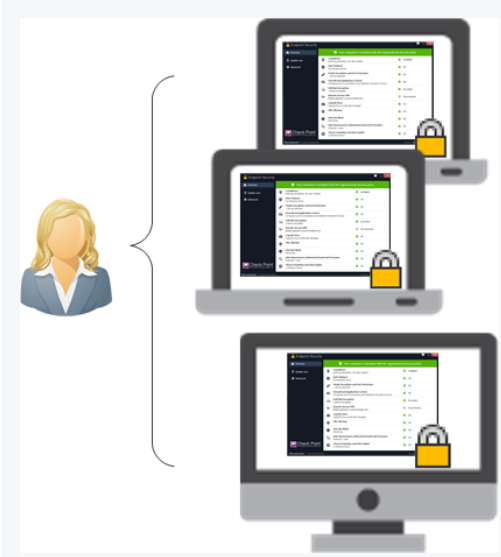
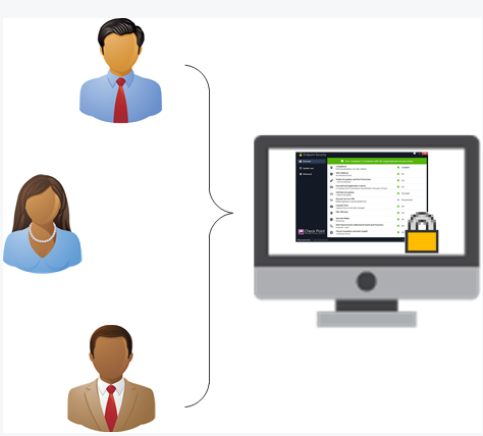
This is the Policy Toolbar:



To do this	Click this
Add and delete rules	
Save, refresh and install policy changes	
Show only the actions that are different than the default rule for that component	
Change the order of the rules for the component. Re-order the rules to define the assignment priority of rules for a specific component	
Search for text and highlight it in the Endpoint Security policy	
Show the policy for a specific part of the organization	

User and Computer Rules

One user may have multiple computers. Some computers may have multiple users.

One user with multiple computers:	One computer with multiple users:
	

The policies for some Endpoint Security components are enforced for each user. See *"Rule Types for Each Endpoint Security Component" on page 171*.

- *User Rules* are independent of computer the user is connected to. However, you can override user rules using *"Virtual Groups in Policy Rules" on page 183*.
- *Computer Rules* are independent of the user who is logged on to the computer.

Connected, Disconnected and Restricted Rules

Endpoint Security can enforce policy rules on computers and users based on their connection and compliance state.

When you create a policy rule, you select the connection and compliance states for which the rule is enforced. You can define rules with these states:

- **Connected** state rule is enforced when a compliant endpoint computer has a connection to the Endpoint Security Management Server. This is the default rule for a component policy. It applies if there is no rule for the Disconnected or Restricted states of the component. All components have a Connected Rule.
- **Disconnected** state rule is enforced when an endpoint computer is not connected to the Endpoint Security Management Server. For example, you can enforce a more restrictive policy if users are working from home and are not protected by organizational resources. You can define a *Disconnected policy* for only some of the Endpoint Security components. See *"Rule Types for Each Endpoint Security Component" on page 171*
- **Restricted** state rule is enforced when an endpoint computer is not in compliance with the enterprise security requirements. In this state, you usually choose to prevent users from accessing some, if not all, network resources. You can define a *Restricted policy* for only some of the Endpoint Security components. See *"Rule Types for Each Endpoint Security Component" on page 171*

Rule Types for Each Endpoint Security Component

The table shows if the policy for each Endpoint Security component is enforced for each user or for each computer (the *Rule Type*).

It is also possible to define a *Connected* policy for all components.

For some components you can also define *Disconnected* and *Restricted* policies.

For instructions on how to change policy type, see the "*Policy Operation*" section in the *R81.20 Harmony Endpoint Web Management Administration Guide*.

Note - Deployment Rules are defined for computers, not for users.

Old Policy Calculation Mode

Component	Rule Type
Full Disk Encryption	Computer only
Media Encryption & Port Protection	Computer (default) or User
OneCheck User Settings	User only
Anti-Malware	Computer (default) or User
Anti-Ransomware, Behavioral Guard and Forensics	Computer only
Anti-Bot and URL Filtering	Computer (default) or User
Threat Emulation, Threat Extraction and Anti-Exploit	Computer (default) or User
Compliance	Computer (default) or User
Firewall	Computer (default) or User
Access Zones	Computer (default) or User
Application Control	Computer (default) or User
Client Settings	Computer (default) or User

Rule Entities

When you configure a rule, you specify the *entities* that the rule *Applies To*.

These are some of the entities you can specify:

- Entire Organization (the root of the organization folders)
- OUs
- Network IP ranges
- AD Groups
- Virtual Groups
- Users (for User Policies only)
- Computers (for Computer Policies only)

Protection for Servers

These components can be installed on supported servers in the same way that they are installed on workstations:

- Anti-Malware
- Firewall
- Compliance

Important -
Application Control is not supported on all versions of Windows Server.
Do not deploy this component on clients that run operating systems that are not supported. You can also disable it in the policy.

To disable components on operating systems that are not supported:

1. Configure a rule that disables the unsupported component.
2. Install the policy on all clients that run operating systems that do not support the component.

If you install Anti-Malware and Firewall policies on servers, it is best for the policies to be machine-based and not user-based. In machine-based policy, the policies assigned to the machine have priority over the policies assigned to users who connect to the machine.

To enforce machine-based policies, we strongly recommend that you put all servers in a server Virtual Group.

For supported servers, see the *Release Notes for your Endpoint Security client version*.

Working With Rules

The policy for each Endpoint Security component is made up of rules.

Each component has a default rule that applies to the **Entire Organization**. You can change the default rule for the component, but you cannot delete it.

For each component, you can add rules that apply to specific parts (entities) of the organization.

- To create a rule, select an existing rule and from the Policy toolbar, click **Create a Rule**
- To create a rule with same settings as an existing rule, right-click the rule and select **Clone Rule**.
- To delete a rule, select the rule, right-click, and select **Delete Rule**.

Creating a Rule

For each component, you can add one or more rules that apply to specific parts (entities) of the organization.

The new rule is added to the bottom of the policy of the component.

To create a rule:

1. Select an existing rule
2. In the Policy toolbar, click **Create a Rule**

   The **Create Rule Wizard** opens.
3. On the **Select Enforcement state** page, select **Add Rule for** and select a state: **Connected**, **Disconnected**, or **Restricted**.

   Endpoint Security can enforce policy rules on computers and users based on their connection and compliance state.

   When you create a policy rule, you select the connection and compliance states for which the rule is enforced. You can define rules with these states:

   - **Connected** state rule is enforced when a compliant endpoint computer has a connection to the Endpoint Security Management Server. This is the default rule for a component policy. It applies if there is no rule for the Disconnected or Restricted states of the component. All components have a Connected Rule.

- **Disconnected** state rule is enforced when an endpoint computer is not connected to the Endpoint Security Management Server. For example, you can enforce a more restrictive policy if users are working from home and are not protected by organizational resources. You can define a Disconnected policy for only some of the Endpoint Security components. See *"Rule Types for Each Endpoint Security Component" on page 171*.
- **Restricted** state rule is enforced when an endpoint computer is not in compliance with the enterprise security requirements. In this state, you usually choose to prevent users from accessing some, if not all, network resources. You can define a Restricted policy for only some of the Endpoint Security components. See *"Rule Types for Each Endpoint Security Component" on page 171*.

4. Click **Next**.
5. On the **Select Entities** page, select those OUs, groups or individuals that this rule applies to.

   To search for an entity: Type text in the field.

   You can add multiple entities.
6. Click **Next**.
7. On the **Change Rule Actions** page, right-click the applicable actions and configure the action.

   Select from a pre-defined action. To create your own, select **Edit Shared Action**.
8. Click **Next**.
9. On the **Edit rule Name and comment** page, enter a descriptive **Name** and optionally **Comment**.
10. Click **Finish**.
11. In the Policy Management Toolbar, click **Install** to install the policy on Endpoint Security clients.

The Order in Which the Client Applies the Rules

If there is more than one rule for an Endpoint Security component, the Endpoint Security client applies the rules in this order:

- First rule that applies to the user or computer in the **more rule(s)** section.
- If no rule matches the user or computer, the *default rule* applies.

Best Practice - Put rules for specified users or computers, in the **more rule(s)** section, above rules for groups and containers they are members of.

Example

Read the comments in the rules.

No	Name	Applies to	Comment
-	**Firewall**		
	Default Firewall settings for the entire organization	**Entire Organization**	This rule applies to users who do not belong to the OUs "Europe" or "US", and do not belong to the AD group "Managers".
-	**2 more rules**		
1	Firewall rule for Europe and US	**Europe** \Directories\example.test.com\Example **US** \Directories\example.test.com\Example	This rule applies to users who belong to the OUs "Europe" and "US".
2	Firewall rule for managers	**Managers** \Directories\example.test.com\Example	This rule applies to users in the AD group "Managers" who do not belong to the OUs "Europe" or "US".

Changing the Order in Which the Client Applies the Rules

When there is more than one rule in the "**more rule(s)**" section, you can change the order in which the Client applies the rules.

To change the order in which the client applies the rules:

1. In the "**more rule(s)**"section, select a rule.
2. In the Policy Toolbar. use the **Move Up** and **Move Down** buttons to change the order of the rule.
3. Click **Save rule**

Example

This is how the Endpoint Security client applies the rules after you change order of the rules in the previous example policy.

If there is more than one rule for an Endpoint Security component, the Endpoint Security client applies the rules in this order:

- First rule that applies to the user or computer in the "**more rule(s)**"section.
- If no rule matches the user or computer, the *default rule* applies.

Best Practice - Put rules for specified users or computers, in the "**more rule(s)**"section, above rules for groups and containers they are members of.

Example 1

Read the comments in the rules.

No	Name	Applies to	Comment
-	**Firewall**		
	Default Firewall settings for the entire organization	**Entire Organization**	This rule applies to users who do not belong to the OUs "Europe" or "US", and do not belong to the AD group "Managers".
-	**2 more rules**		
1	Firewall rule for Europe and US	**Europe** \Directories\example.test.com\Example **US** \Directories\example.test.com\Example	This rule applies to users who belong to the OUs "Europe" and "US".
2	Firewall rule for managers	**Managers** \Directories\example.test.com\Example	This rule applies to users in the AD group "Managers" who do not belong to the OUs "Europe" or "US".

Example 2

Read the comments in the rules.

No	Name	Applies to	Comment
-	**Firewall**		
	Default Firewall settings for the entire organization	**Entire Organization**	This rule applies to users who do not belong to the OUs "Europe" or "US", and do not belong to the AD group "Managers".
-	**2 more rules**		
1	Firewall rule for managers	**Managers** \Directories\example.test.com\E...	This rule applies to users in the AD group "Managers".
2	Firewall rule for Europe and US	**Europe** \Directories\example.test.com\Example **US** \Directories\example.test.com\Example	This rule applies to users who belong to the OUs "Europe" and "US" who are not in the AD group "Managers".

Editing a Rule

You can modify a rule in the **Policy** tab. You can change the:

- **Name**
- Entities that the rule **Applies To**. However, you cannot change the entities in a default rule. The default rule applies to the Entire Organization.
- **Actions - Best practice** is to not change predefined actions. If you want to change a setting, create a custom action.
- **Comment**

To edit name or comment of a rule:

Double-click the text in the name or comment of the rule, and modify it.

To add an entity to a rule:

1. In the **Applies To** column of the rule, click **Add Assignment**
2. Click ...
3. Select the entity from the organizational tree.

To remove an entity from a rule:

In the **Applies To** column of the rule, select the entity and click **Remove**

To edit an action of a rule:

If you edit an action that is used in more than one rule (a shared action), the change applies everywhere that the rule is used.

Editing a Shared Action

You can edit an action in these ways:

Edit a Shared Action	A Policy action can be used in more than one rule. That is why it is called a *Shared Action*. **Important** -If you *edit a shared action*, the change applies everywhere the action is used. For example, if you change an action that is used in rule A and in rule B, the change happens in both rules.
Clone an Action	If an action is used in more than one rule and you want to change the action in one rule and not the others, *clone the action*. Then, use the cloned action in one of the rules, and changed the settings of the cloned action. You can use the cloned action in more than one rule. *Custom actions* show below the predefined actions
Use a Predefined Action	Many actions have more than one predefined setting You can easily change the action by selecting a different predefined setting.

Best Practice - Do not change predefined actions. If you want to change a setting, create a custom action.

To edit a rule action:

1. In the Policy rule, click the action.
2. Edit the action in one of these ways:
   - **Edit Shared Action** to edit the properties of the action. Changes affect all the rules that use the action.
   - **Clone Action** to create a custom action.
   - Select a different predefined action.

To find out where an action is used:

1. In the Policy rule, click the action.
2. Click **Edit Shared Action**.
3. In the **Description** section, look for the Wide Impact Icon  Used in 3 rules
4. Click the *Used in N rules* link to see where the action is used.

What Happens when you Delete an Entity

If an entity is deleted - for example, an Active Directory group, user or computer - and there is a rule for the deleted entity:

- The rule is automatically moved to a section of the component policy called **Rule with no assignments**.
- The **Applies To** column shows  **Deleted Entities**.

To restore a rule with a deleted entity:

1. Right-click the rule and select **Restore Rule**.
2. Select new entities for the rule.

Saving and Installing Policy Changes on Clients

When you create or modify a rule, you have to save it and install it before becomes available to the Endpoint Security clients.

This lets you save changes to the Policy without immediately affecting users. It also lets you deploy the Policy at the most convenient time, for example, at night.

The policy becomes available for endpoints to download on the next heartbeat or the next time user logs in.

Changes to Virtual Groups

If you make changes to an object that is related to Virtual Groups, the changes are enforced immediately. For example, if you move an object into a virtual group, the rules for that group apply to the object immediately. However, if you change a policy that is assigned to a virtual group, the changes to the policy only apply after you install policies.

To save a rule:

- Select a rule, and in the **Policy** tab, click **Save rule**.

  or

- Select a rule, and from the **File** menu, select **Save**.

To install the Policy on Endpoint Security clients:

- In the **Policy** tab, click **Install**.

  or

- From the **File** menu, select **Install Policies**.

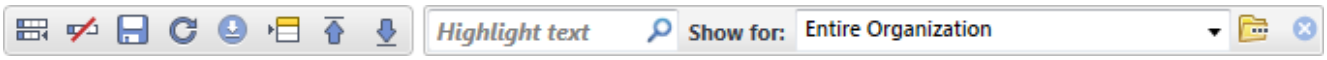
Showing the Policy that Applies to a User or Computer

By default, the Policy tab shows default rules that apply to **Entire Organization**, and other rules that apply to other entities.

You can filter the view in the Policy tab and show the Policy for a specific part of the organization.

To show the Policy for a specific part of the organization:

In the **Policy** tab, in the **Show for** area of the toolbar, type the name of a user, computer, OU, or other entity.



If you show the Policy for a specific user, you can select the associated computer.

You cannot edit the policy when list is filtered

To restore the default view and show the entire Policy, click **Clear**.

Direct Assignment of Rules to Users and Computers

You can assign rules to an entity. This is called *Direct Assignment*. You can also see which rules are assigned to an entity.

To assign a rule to an entity:

1. Open the **Users and Computers** tab.
2. In the **All Organization Folders** area, search for the entity
3. In the **Blades** area, select a component.
4. In the **Rule** area, review the rule that is assigned to the entity for this component.
5. To change the rule specifically for the entity, click **Edit rule**.
6. In the **Edit Specific Rule** page, select **Differentiate <name of entity>**.
7. Click **Next**.
8. In the **Change rule action settings** page, Select the actions you want to change, and change the settings.
9. Click **Next**.
10. In the **Enter rule name and comment** page, add the details.
11. Click **Finish**.
12. Click **Save**.

Review the rule that is assigned to the entity for this component. Notice that **Inherited From** shows *Direct Assignment*. In the **Policy** tab, you can see the new component rule for the entity.

To remove direct assignment from an entity:

1. Open the **Users and Computers** tab.
2. In the **All Organization Folders** area, search for the entity
3. In the **Blades** area, select a component.
4. In the **Rule** area, review the rule that is assigned to the entity for this component. **Inherited From** shows *Direct Assignment*.
5. Click **Remove Direct Assignment**.
6. Click **Yes**.

Review the rule that is assigned to the entity for this component. Notice that **Inherited From** shows *Entire Organization*. In the **Policy** tab, the component rule for the entity has been deleted.

Virtual Groups in Policy Rules

You can use these types of groups in SmartEndpoint:

- *Active Directory group* - These are synchronized automatically from Active Directory using the Directory Scanner. You cannot modify an Active Directory group.
- Virtual group - Create these in SmartEndpoint or use one of the predefined virtual groups. There are two types of virtual group:
  - *Virtual Group* - Can contain users and computers.
  - *Computer Group* - Can contain only computers.

Virtual Groups work like Active Directory groups. You can:

- Create groups and then add users and computers to the groups automatically or manually.
- Assign policies to virtual groups or users.
- Put users and computers into more than one group.
- Select which policies have priority for endpoints that belong to more than one virtual group.

You can use Virtual Groups with Active Directory for added flexibility or as an alternative to Active Directory.

Members of Active Directory OUs or groups can also be members of Virtual Groups.

Important - You can use virtual groups to manage computers and servers in all environments. To manage users with a virtual group, you must do one of these steps:

- Use Full Disk Encryption and enable **User Acquisition**.
- Import objects into Endpoint Security with the Active Directory Scanner. Then, you can move them between virtual groups manually.

For each Endpoint Security component, only one rule can be assigned to a user or computer. Therefore, if a user belongs to more than one group, with a different rules assigned to each group, the Endpoint Security Management Server applies the first rule that matches the users or computer.

Why Use Virtual Groups

You may want to use Virtual Groups if you are:

- Using Active Directory but do not want to use it for Endpoint Security. For example:
  - Different administrators manage the Active Directory and Endpoint Security.
  - Your Endpoint Security requirements are more complex than the Active Directory groups. For example, you want different groups for laptop and desktop computers.
- Using a non-Active Directory LDAP tool.
- Working without LDAP.
- Creating computer-based policies for Endpoint Security components that normally support only user-based Policies.

Prerequisites for Using virtual groups

Important - To manage *users* with a virtual group, you must do one of these steps:

- Use Full Disk Encryption and enable *"User Authorization before Encryption" on page 229*.
- Import objects into Endpoint Security with the Active Directory Scanner. Then, you can move them between virtual groups manually.

Types of Virtual Groups

There are two types of virtual groups:

- **Virtual Group** - Can contain users and computers.
- **Computer Group** - Only contains computers. Computers in this group have computer-based policies if there is a policy assigned to the group. The priority of the policies is based on the sequence of rules in the Policy Rule Base.

  For example, Media Encryption & Port Protection policy rules normally apply to users, regardless of which endpoint computer they use. However, if a Media Encryption & Port Protection rule is applied to a Computer Group, that rule can be effective before a rule that applies to a user. This is true if the Computer Group rule is above the user's rule in the Policy Rule Base.

If you add objects to a virtual group with an installation package, the objects are not automatically put into these virtual groups. You must do so manually. See *"Adding Objects with an Installation Package" on page 188*,

Predefined Virtual Groups

Users and computers with Endpoint Agent installed are automatically assigned to these predefined virtual groups:

- **All Laptops**
- **All Desktops**

- **All Servers**
- **All Mac OS X Desktops**
- **All Mac OS X Laptops**
- **All Windows Desktops**
- **All Windows Laptops**

The users and computers can be added to another virtual group, or removed from a virtual group and added to another virtual group.

If you add objects to a virtual group with an installation package, the objects are not automatically put into these virtual groups. You must do so manually. See .

Managing Virtual Groups

Work with virtual groups in the **Virtual Group** branch of the **Users and Computers** tree.

When you create a new virtual group, you set the group type, which you cannot change. Changes to a virtual group are saved automatically and installed immediately on the Endpoint Security clients.

- A user or a computer can belong to multiple virtual groups
- Only computers can be added to Computer virtual groups
- You can copy users and computers to other virtual groups.
- You can remove users and computers from a virtual group
- You can copy Active Directory users, computers and members of Active Directory groups to a virtual group.

Assign the Virtual Groups in a Policy rule, as for any other entity.

To create a new virtual group:

1. In the **Users and Computers** tree, click **Global Actions** > **New Virtual Group**.
2. In the **New Virtual Group** window:
    - Enter a name for the group.
    - Optional: Enter a **Comment**.
    - Select **Virtual Group** or **Computer Group**.
3. Click **Next**.
4. In the **Select Entities** window, select the members of the group.
5. Click **Finish**.

To add computers and users from Active Directory to a Virtual Group:

1. Right-click an OU on the **Directories** branch of the **Users and Computers** tree.
2. Select **Add content to Virtual Group**.
3. Select a Virtual Group and click **OK**.

   All users and computers in the specified OU are added to the Virtual Group.

   If select one of the default Virtual Groups, only those users and computers applicable to that group are added. For example, if you select the All Laptops Virtual Group, only laptops computers and their users are added to the group.

To copy a user or computer to another virtual group:

1. Right-click the user, computer or Active Directory group.
2. Select **Add to Virtual Group**.
3. Select the destination virtual group.

The source object becomes a member of the destination group while remaining a member of the source group.

To remove a user or computer from a virtual group:

1. Right-click the user or computer.
2. Select **Remove from Virtual Group**.

Using a Computer Group in a User-Based Policy

You can assign a rule to a Virtual Group, as you can for any other entity.

This example shows how to use a Computer Group in the Media Encryption & Port Protection Policy, which is user-based.

Best Practice - In a component policy that is user-based, put computer group rules above user rules in the "more rule(s)" section

Read the comments in the rules.

No	Name	Applies to	Comment
-	**Media Encryption & Port Protection**		

No	Name	Applies to	Comment
	Default Media Encryption & Port Protection settings for the entire organization	**Entire Organization**	This rule applies to all users that are not logged into computers in "Media Encryption computer Group"
-	**1 more rule**		
1	Media Encryption & Port Protection Rule for "Media Encryption computer Group"	**Media Encryption computer Group** \Virtual Groups	Media Encryption & Port Protection policy rules normally apply to users, regardless of which endpoint computer they use. However, this rule applies to computers in "Media Encryption Computer Group" regardless of which users are logged in to the computer.

Example Deployment Rules for Virtual Groups

You can deploy Endpoint Security components to Endpoint Security clients according to Virtual Groups.

This example shows Software Deployment Rules that specify the components to be deployed to the *All Laptops* and *All Desktops* Virtual Groups.

Read the comments in the rules.

No	Name	Applies to	Actions	Comment
-	**Software Deployment**			
	Default Deployment	Entire Organization	Do Not install	Default Software Deployment settings for the entire organization
-	**2 more rules**			
1	Deployment to Desktops	All Desktops \Virtual Groups	Endpoint Client Version 80.88.4122 Selected blades	

No	Name	Applies to	Actions	Comment
2	Deployment to laptops	All Laptops \Virtual Groups	Endpoint Client Version 80.88.4122 Selected blades	Same as desktop plus Full Disk Encryption and Endpoint Security VPN

Adding Objects with an Installation Package

When you distribute a new Endpoint Security client installation package, you can assign users and computers to a destination group. Computers and users that use this package are automatically assigned to the group when they connect to the server for the first time.

For example, an MSP that services 5 organizations can export 5 installation packages to divide endpoints into 5 different groups. Users who install the package designated for Group A are automatically put in Group A. Users who install the package designated for Group B are automatically put in Group B.

To configure a virtual group destination for an installation package:

1. In the **Users and Computers** tab, create a virtual group.
2. In the **Deployment** tab, click **Packages for Export**.
3. Select a package and change the rule settings to **Export to** the new virtual group.

   Change other rule settings as necessary. If you are upgrading from version R73 or earlier, make sure that you configure the legacy version passwords.
4. Right-click the package and select **Export Package** from the option menu.
5. In the **Export Package** window, select the platform type and 32-bit or 64-bit.
6. Define the path to the directory that the package is saved to.
7. Click **OK**.

   The package downloads to the specified location.

Monitoring Virtual Groups

Virtual Groups show in Reporting reports like other objects. You can create for monitoring and other purposes. Endpoints can be members of more than one group.

For example, if you want to do a test of a new Endpoint Security upgrade, you can create a Virtual Group that contains only those endpoints included in the test. Then you can create a report for the deployment and activity of these endpoints.

To see activity for virtual group objects:

1. Go to the **Reporting** tab and select **Software Deployment** from the tree.
2. Click the **...** button in the **Endpoint List** section of the **Software Deployment Status** pane.
3. Select **Virtual Groups** and then the select the virtual group that you want to see.

External Endpoint Policy Servers

If no external Endpoint Policy Servers are configured, the Endpoint Security Management Server, which contains an Endpoint Policy Server, manages all client requests and communication.

If you install more Endpoint Policy Servers, they manage most communication with the Endpoint Security clients. This keeps the Endpoint Security Management Server more available for other tasks. If you configure the Endpoint Security Management Server to behave as an Endpoint Policy Server in addition to other Endpoint Policy Servers, the work of communication with the clients is distributed to them all.

Installing and Configuring an Endpoint Policy Server

We recommend that you use a distributed deployment that contains external Endpoint Policy Servers on dedicated computers.

- Install at least one Endpoint Policy Server for each remote site.
- For larger sites, install many Endpoint Policy Servers to improve performance.

An Endpoint Policy Server is a Log Server that you configure as an Endpoint Policy Server.

Installing an Endpoint Policy Server

To install Endpoint Policy Server, install a Log Server and configure it as Endpoint Policy Server. Use the instructions in the *R81.20 Installation and Upgrade Guide*.

Configuring an Endpoint Policy Server

To define an Endpoint Policy Server:

1. In SmartEndpoint, go to **Manage > Endpoint Servers**.

   The **Endpoint Servers** window opens.

2. Click **New**.

   To edit an existing server, select it from the list and click **Edit**.

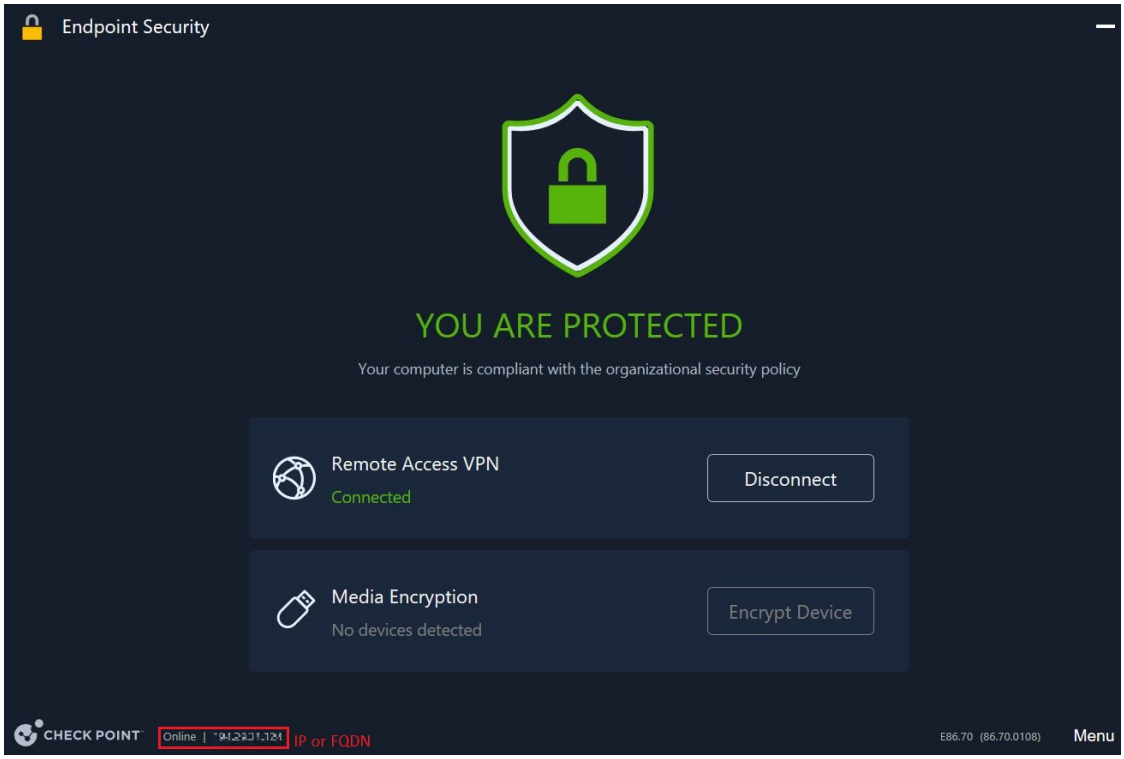
   The **Endpoint Server Wizard** opens.

3. In the **Name** field, enter the Fully Qualified Domain Name (FQDN) of the Endpoint Policy Server. For example, *somehost.example.com.*

Note - We recommend that you enter the FQDN so that if the IP address of the server changes, the client uses the FQDN to communicate with the server. It also allows you to use an internal non-routable, private IP address for the server (for example 10.1.2.3).

4. In the **IP Address** field, enter the IP address of the Endpoint Policy Server.

   Note - The Harmony Endpoint Security Client uses either FQDN or IP address, whichever is quicker to communicate with the server and displays it in the Endpoint Security Client Home screen.



5. Select **Endpoint Policy Server**
6. Click **Next**.
7. Select an option to initiate secure trusted communication now or later:
   - **Initiate trusted communication** (If the servers are up and able to communicate)
     - Enter and confirm an **Activation Key**. You will enter this same key on the other servers.
     - Click **Initialize**.
   - **Skip and initiate trusted communication later** (If the servers are not ready to communicate)
8. Click **Next**.

   A warning pop-up window shows.
9. Click **OK**.

10. Click **Finish**.

    The **Install Database** window opens.

11. Wait for the database installation to finish.

    The **Close** button becomes available.

12. To verify if your server in an Endpoint Policy Server or an Endpoint Management Server:

    a. Connect to the server using SSH.

    b. Run :

    ```
    cpprod_util UepmIsPolicyServer
    ```

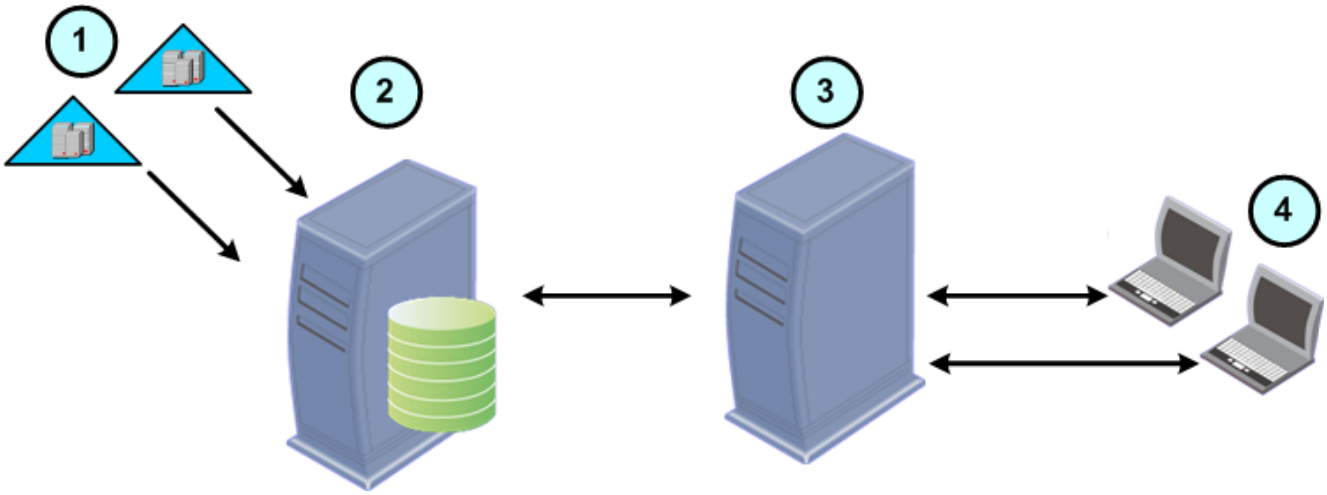
    The output **1** indicates that your server is an Endpoint Policy Server and the output **0** indicates that your server is an Endpoint Management Server

How do Endpoint Policy Servers Work?

External Endpoint Policy Servers decrease the load of the Endpoint Security Management Server and reduce the bandwidth required between sites. By default, the Endpoint Security Management Server also acts as an Endpoint Policy Server, in addition to the other Endpoint Policy Servers. The work of communication with the Endpoint Security clients is distributed among all of them.

The Endpoint Policy Servers are located between the Endpoint Security clients and the Endpoint Security Management Server. For most tasks, Endpoint Security clients communicate with the Endpoint Policy Servers and the Endpoint Policy Servers communicate with the Endpoint Security Management Server.

If there are multiple Endpoint Policy Servers in an environment, each Endpoint Security client does an analysis to find which Endpoint Policy Server is "closest" (will be fastest for communication) and automatically communicates with that server.



Item	Description
1	Active Directory Domains
2	Endpoint Security Management Server
3	External Endpoint Policy Server
4	Enterprise workstations with Endpoint Security clients installed

The Endpoint Policy Server handles the most frequent and bandwidth-consuming communication. The Endpoint Policy Server handles these requests without forwarding them to the Endpoint Security Management Server:

- All heartbeat and synchronization requests.
- Policy downloads

- Dynamic (EXE) and Windows installer (MSI) package downloads
- Anti-Malware updates
- All Endpoint Security client logs (the Endpoint Policy Server is configured as Log Server by default).

The Endpoint Policy Server sends this data to the Endpoint Security Management Server:

- All component-specific messages (which require information to be stored in the database). For example, Full Disk Encryption recovery data.
- Monitoring data. This includes the connection state and other monitoring data for connected clients.
- Policy Server generated messages.

Configuring Policy Server Settings

The primary aspects of working with Endpoint Policy Servers that you can configure are:

- The interval after which the clients do an analysis to choose which Endpoint Policy Server to connect to.
- If the Endpoint Security Management Server also behaves as an Endpoint Policy Server or not.

Endpoint Policy Server Proximity Analysis

In a large network, multiple Endpoint Policy Servers can be available for an endpoint client. In such an environment, the client does an analysis from a list of Endpoint Policy Servers to find the server closest to it. The client sends a specified HTTP request to all Endpoint Policy Servers on the list. The server that replies the fastest is considered to be closest.

The server list is an XML file named `epsNetwork.xml`. It is located at `$UEPMDIR/engine/conf/` on the Endpoint Security Management Server. It contains:

- The topology of Endpoint Policy Servers on the network that Endpoint Security clients can connect to.
- Protocols, authentication schemes, and ports for each message passed between client and server.

How the proximity analysis works:

1. The Endpoint Security Management Server creates a list of Endpoint Policy Servers based on the servers configured in the SmartEndpoint.
2. The Endpoint Security Management Server pushes the list to the clients.
3. The Device Agent on the client does a proximity analysis after a specified interval to find the Endpoint Policy Server 'closest' to it. Some events in the system can also cause a new proximity analysis. Proximity is based on the response time of a specified HTTP request sent to all servers on the list.

   Note - Proximity is not based on the physical location of the server. A client in New York will connect to the California Endpoint Policy Server if the California Endpoint Policy Server replies before the New York Endpoint Policy Server.
4. The client tries to connect to the closest Endpoint Policy Server.
5. If a server is unavailable, the Device Agent tries the next closest server on the list until it makes a connection.
6. Based on data contained in the shared list, the client and Endpoint Policy Server create connection URLs.

Clients continue to connect to the closest Endpoint Policy Server until the next proximity analysis.

Note - You cannot figure which particular Endpoint Policy Servers a client should use, only a list of servers for the client to choose from.

Configuring Endpoint Policy Server Connections

To configure Endpoint Policy Server connections:

1. From SmartEndpoint menu, select **Manage** > **Endpoint Connection Settings**.
2. Enter or select the **Interval between client heartbeats** value (Default = 60 seconds). See *"The Heartbeat Interval" on page 391*.
3. Enter or select the **Client will re-evaluate the nearest Policy Server after** value (default = 120 minutes).

   This value is the interval, in minutes, after which endpoint clients search for the closest available Endpoint Policy Server.
4. **Optional**: Select **Enable Endpoint Security Management Server to be the Endpoint Policy Server**.

   This option includes Endpoint Security Management Servers in the search for the closest Endpoint Policy Server.
5. Enter or select the **Client will restrict non-compliant endpoint after** value (default = 5 heartbeats). See *"The Heartbeat Interval" on page 391*.
6. Click **OK**.
7. Install policies to endpoint computers.

Enabling the Management Server to be an Endpoint Policy Server

Configure if the Endpoint Security Management Server behaves as an Endpoint Policy Server along with the other Endpoint Policy Servers.

The default is that the Endpoint Security Management Server does behave as an Endpoint Policy Server.

Note - If you do not explicitly enable the Endpoint Security Management Server to behave as an Endpoint Policy Server, it is still in the proximity analysis list. If no other Endpoint Policy Servers can reply to a client, the Endpoint Security Management Server replies.

To configure the Endpoint Security Management Server to behave as an Endpoint Policy Server only if all Endpoint Policy Servers do not respond:

1. In SmartEndpoint, select **Manage** > **Endpoint Connection Settings**.
2. Clear **Enable Endpoint Management Server to be Endpoint Policy Server**.
3. Click **OK**.
4. Select **File** > **Install Policies** or click the **Install Policies** icon.

Policy Server and Management Server Communication

The communication between the Endpoint Security Management Server and the Endpoint Policy Servers includes:

- Endpoint Policy Servers get from the Endpoint Security Management Server:
  - Policies and installation packages.
  - All files that it needs for synchronization.
- Endpoint Policy Servers send a heartbeat message to the Endpoint Security Management Server at 60 second intervals.

  You can change this in the `$UEPMDIR/engine/conf/global.properties` file on the Endpoint Security Management Server. The property name is `connectionpoint.hb.interval.secs`.
- Endpoint Policy Servers send sync messages to the Endpoint Security Management Server when synchronization is necessary.
- Endpoint Policy Servers send Reporting events to the Endpoint Security Management Server at 60 second intervals or when there are more than 1000 events in the queue.

  You can change this in the `$UEPMDIR/engine/conf/global.properties` file on the Endpoint Security Management Server. The property names are:
  - `connectionpoint.emon.events.until.flush=1000`
  - `connectionpoint.emon.seconds.until.flush=60`
- Endpoint Policy Servers send all database related messages directly to the Endpoint Security Management Server.

Notes on the First Synchronization

After you create the Endpoint Policy Server and install the policy in SmartEndpoint, the first synchronization between the Endpoint Policy Server and Endpoint Security Management Server occurs. During the first synchronization, the Endpoint Policy Server does not handle endpoint requests and shows as **Not Active** in the Reporting tab.

The first synchronization can take a long time, based on the amount of policies and installation packages that the Endpoint Policy Server must download from the Endpoint Security Management Server.

When the first synchronization is complete, the Endpoint Policy Server will show as **Active** in the Reporting tab.

Configuring an Alert for a Non-Synchronized Policy Server

You can configure the Endpoint Security Management Server to send an email alert to one or more people if one or more of the Policy Servers are not synchronized with the Endpoint Security Management Server.

It is important for all the Endpoint Policy Servers to have the same information about the Endpoint Security Management Server, because if they are not synchronized, the environment may be in a non-stable state.

You can configure how often the Endpoint Security Management Server sends the Policy Server out-of-sync alert, and whether it sends an alert when the Policy Server is back in sync.

Before Configuring a Policy Server Out-of-Sync Alert

Configure an email server (see *"Configuring an Email Server" on page 68*).

To Configure a Policy Server Out-of-Sync Alert:

1. In SmartEndpoint, go to the **Reporting** tab.
2. In the **Alerts** section, click **Policy Server out of sync**.
3. Enable the alert so that it is **ON**.
4. Click **Configure**.

   The **Alert Configuration** window opens.
5. Add one or more people who will get an email about the alert. In **Add New Recipient**, for each person you want to add, type an email address and click **Add**.
6. Configure when an alert is sent. Select one or two of:
   - **Notify on alert activation** - Email alert is sent when the Policy Server is out of sync.
   - **Notify on alert resolution** - Email alert is sent when the Policy Server is back in sync.
7. Set how often the alert will be sent. In **Remind every**, select one of these time periods:

   1 Day

   1 Hour

   6 Hours

   3 Days

1 Week

None

8. Click **OK**.

Example Alert Email About Policy Server Out-of-Sync

This is an example of an alert mail that the Endpoint Security Management Server sends when an Endpoint Policy Server becomes out-of-sync.

```
This is an automated message about Active Alerts from the
Endpoint Security Management server.
This alert is active:
Policy Server Out of Sync Alert

Number of inactive Policy servers: 1 out of 1

The list of inactive Policy servers: [ps3 (192.0.2.17) ]

For more information, see the  Endpoint Security Management
console in Reporting > Activity Reports > Endpoint Policy Servers
Status.
```

Monitoring Endpoint Policy Server Activity

You can see the status of Endpoint Policy Servers in the **Reporting** tab of SmartEndpoint.

In the **Reporting** tab, select **Endpoint Policy Servers Status**.

- In the **Status** list, select which Endpoint Policy Servers to see:
  - **All**.
  - Only **Active**.
  - Only **Not Active**.
- In the table see:
  - **Name** - The name of the server in SmartEndpoint.
  - **IP Address** - The IP Address entered for the server.
  - **DN** - Its full DN name, taken from SmartConsole.
  - **Active** - If the server is **Active** or **Not Active**. Active means that the server recently sent a heartbeat message.
  - **Last Contact** - When the Endpoint Security Management Server last received a heartbeat message from it.
  - **Comments** - Comments written for that server in **Properties** window.

For more detailed information, you can look at the log messages on the Endpoint Policy Server. They are in: `$UEPMDIR/logs`

You can see if there are errors in the logs and resolve them if necessary.

Management High Availability

High Availability is redundancy and database backup for management servers. Synchronized servers have the same policies, rules, user definitions, network objects, and system configuration settings. The first management server installed is the primary. If the primary Security Management Server fails, or is off line for maintenance, the secondary server takes over.

When you use Check Point Endpoint Security, the Endpoint Security Management Server is fully integrated with the Network Security Management Server on the same computer. This means that the Security Management High Availability solution supplies backup and redundancy for the Network Security Management Server and the Endpoint Security Management Server databases.

Only one Secondary server is supported with Endpoint Security.

To learn how to configure and manage a High Availability environment, see "Management High Availability" in the *R81.20 Security Management Administration Guide*.

Information that is different for environments with Endpoint Security is included in this guide.

Environments that include Endpoint Security require some additional steps for:

- Configuring a secondary server
- Failover
- Synchronization of MSI files and drivers

Configuring a Secondary Server

To add a secondary server for an Endpoint Security environment, you must follow the workflow defined here. You must create communication between the servers and install the database BEFORE you enable Endpoint Security. After the first database installation and synchronization are completed, you enable Endpoint Security with the **Endpoint Policy Management** component, and then install the database again.

To add a secondary server and establish communication between the servers:

1. Install a new Security Management Server.
2. In SmartConsole, connect to the primary server.
3. Create a network object for the secondary server: In the **Gateways & Servers** tab, click the **New** icon and select **Network Objects** > **Gateways and Servers** > **Check Point Host**.

4. In the **General Properties** page of the window that opens, enter a unique name and an IP address for the server.
5. In the **Management** tab of the **General Properties** page, select **Network Policy Management**.

   Secondary Server, **Logging & Status**, and **Provisioning** are selected automatically

   DO NOT enable Endpoint Policy Management on the server.
6. Click **Communication** to create SIC trust between the Secondary Endpoint Security Management Server and the Primary Endpoint Security Management Server.
7. In the window that opens enter these configuration parameters:
   - **One-time password** (twice to confirm) - SIC Activation Key that you entered in the Check Point Configuration Tool
   - Click **Initialize** to create a state of trust between the Endpoint Security Management Servers. If the trust creation fails, click **Test SIC Status** to see troubleshooting instructions
   - If you must reset the SIC, click **Reset**, then reset the SIC on the Secondary server and click **Initialize**.
8. Click **Close**.
9. Click **OK**.
10. From the menu, select **Install Database**.
11. Wait for the peer initialization and the full sync with peer to finish.

To enable Endpoint Security on the secondary server:

1. After the previous procedure is completed, in SmartConsole, open the secondary server object.
2. In the **Management** tab of the **General Properties** page, select **Endpoint Policy Management**.
3. Click **OK**.
4. Select **File** > **Save**.
5. From the menu, select **Install Database**.
6. Follow the steps in *"Synchronizing MSI Files, Dynamic Packages and Drivers" on the next page*.

Synchronizing MSI Files, Dynamic Packages and Drivers

Each time you download a new MSI package, Dynamic Package or a driver related to Endpoint Security client, for example, a Smart Card driver, you must manually synchronize these files in all the High Availability environments. The synchronization is not performed automatically due to large file size.

To synchronize MSI Files, Dynamic Packages and Drivers:

1. Manually copy the MSI folder to the Standby servers.

   Note: The MSI folder contains many folders with unique names. When you add a new file to a folder on the Active server, copy this file to the same folder on the Standby server.

   a. On the Active Security Management Server, copy these folders:

      - `$FWDIR/conf/SMC_Files/uepm/msi`
      - `$FWDIR/conf/SMC_Files/uepm/packages`
      - `$FWDIR/conf/SMC_Files/uepm/recimg`
      - `$FWDIR/conf/SMC_Files/uepm/archives`

   b. On the Standby Security Management Server, replace theses folders with the folders that you copied from the Active Security Management Server:

      - `$FWDIR/conf/SMC_Files/uepm/msi`
      - `$FWDIR/conf/SMC_Files/uepm/packages`
      - `$FWDIR/conf/SMC_Files/uepm/recimg`
      - `$FWDIR/conf/SMC_Files/uepm/archives`

   c. If necessary, manually copy the Smart Card drivers:
   `$FWDIR/conf/SMC_Files/uepm/DRIVERS`

d. Run:

i. `cd $FWDIR/conf/SMC_Files/uepm`

ii. `chmod -R u+rwx,g+rwx,0-rwx msi/`

iii. `chmod -R u+rwx,g+rwx,0-rwx packages/`

iv. `chmod -R u+rwx,g+rwx,0-rwx recimg/`

v. `chmod -R u+rwx,g+rwx,0-rwx archives/`

vi. `find msi/ -type d -exec chmod g+s {} \;`

vii. `find packages/ -type d -exec chmod g+s {} \;`

viii. `find recimg/ -type d -exec chmod g+s {} \;`

ix. `find archives/ -type d -exec chmod g+s {} \;`

2. On the Standby Security Management Server, replace theses folders with the folders that you copied from the Active Security Management Server: `$FWDIR/conf/SMC_Files/uepm/DRIVERS`

Online Automatic Sync

In R80.10 and higher, the Endpoint Security database uses online synchronization. Online synchronization synchronizes the Endpoint Security Management Servers each time the database is modified.

Online synchronization is supported on Gaia servers only.

To check the status of the first synchronization:

Run this command on each server:
`PgOnlineSyncUtil is_initial_load_over`

When the synchronization finishes, the command output is
`Initial load is over.`

Before Failover

Whenever possible, change the Active Endpoint Security Management Server to Standby before you change the Standby Endpoint Security Management Server to Active, and check online synchronization status on the Secondary server and all Remote Help servers.

Notes -

- A standby Endpoint Security Management Server cannot be changed to Active until the first synchronization of the Endpoint Security database is completed.
- While the Primary server is offline and the Secondary server is active, external Remote Help servers do not get updates.

Database Migration in a High Availability Environment

If a High Availability configuration was exported, you must re-configure it after the import.

Best practice is to re-install all Secondary Servers and Remote Help Servers after the migrate import procedure.

Install new Secondary Servers and Remote Help Servers of the same version as the primary server and synchronize all servers.

Updating the PAT Version on the Server

When you change a Standby Security Management Server to Active, the new Active Security Management Server can have an older Policy Assignment Table (PAT) version than the clients. If the PAT version on the server is lower than the PAT version on the client, the client will not download policy updates.

To fix this, update the PAT number on the Active server.

To get the PAT version:

If the Active Security Management Server is available, get the last PAT version from it.

On the Active Server:

Run: `uepm patver get`

If the Active Security Management Server is not available, get the last PAT version from a client that was connected to the server before it went down.

On the client computer:

1. Open the Windows registry.
2. Find `HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\EndPoint Security\Device Agent`
3. Double-click the **PATVersion** value.

The **Edit String** window opens.

4. Copy the number in the **Value data** field. This is the PAT version number.

To change the PAT version on the server:

1. Open a command prompt.
2. Run the Endpoint Security Management Security utility (`uepm.exe`) and set the new PAT version:

   ```
   uepm patver set <old_PAT_version_number> + 10
   ```

3. Make sure the new PAT version is set by running:

   ```
   uepm patver get
   ```

Deleting a Server

You can delete a Remote Help server or a Secondary Endpoint Security Management Server. Before you do that, make sure none of the remaining servers have connectivity to the deleted entities.

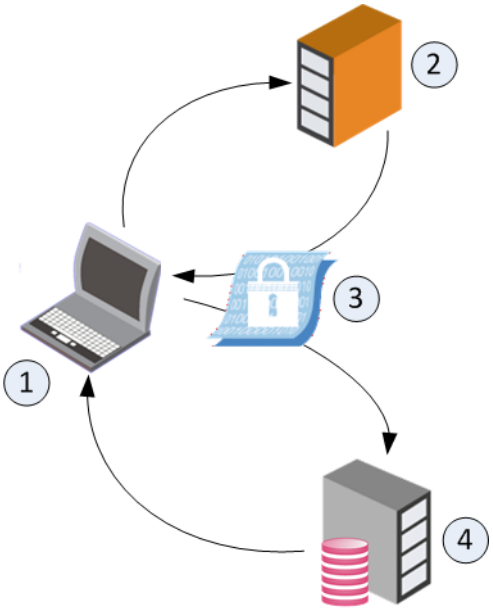
Active Directory Authentication

Endpoint Security Active Directory Authentication

When an Endpoint Security client connects to the Endpoint Security Management Server, an authentication process identifies the endpoint client and the user currently working on that computer.

The Endpoint Security system can function in these authentication modes:

- **Unauthenticated** mode - Client computers and the users on those computers are not authenticated when they connect to the Endpoint Security Management Server. They are trusted "by name". This operation mode is recommended for evaluation purposes only.
- **Strong Authentication** mode - Client computers and the users on those computers are authenticated with the Endpoint Security Management Server when they connect to the Endpoint Security Management Server. The authentication is done by the Active Directory server using the industry-standard Kerberos protocol. This option is only available for endpoints that are part of Active Directory.



The authentication process:

1. The Endpoint Security client (1) requests an authentication ticket from the Active Directory server (2).
2. The Active Directory server sends the ticket (3) to the client (1).
3. The client sends the ticket to the Endpoint Security Management Server (4).

4. The Endpoint Security Management Server returns an acknowledgment of authentication to the Endpoint Security client (1).

The default behavior after Security Management Server installation is **Unauthenticated** mode. It is recommended that you use this mode when you are evaluating Endpoint Security, in a lab environment. Change to **Strong Authentication** mode just before moving to a production environment. It is not recommended to continue to work in **Unauthenticated** mode after moving to production in a live environment.

Important - If you use Active Directory Authentication, then Full Disk Encryption and Media Encryption & Port Protection are only supported on endpoint computers that are part of Active Directory.
Note - If you have endpoint computers in your environment that are not part of Active Directory, Full Disk Encryption and Media Encryption & Port Protection will not work on them.

Configuring Active Directory Authentication

Make sure you configure Strong Authentication for your production environment. Do not set up Strong Authentication before you are ready to move to production. When you are ready to move to production, follow this process.

Workflow for Configuring Strong Authentication:

Step 1 of 3: Configuring the Active Directory Server for Authentication

Endpoint Security Strong Authentication uses the Kerberos network authentication protocol.

To enable the Active Directory server to validate the identity of clients that authenticate themselves through Kerberos, run the `ktpass.exe` command on the Active Directory Server. By running the `ktpass` command, you create a user that is mapped to the `ktpass` service. This creates a *Principal Name* for the AD server. The Principal Name must have the following format: `ServiceName/realm@REALM`

Important - After you create the user that is mapped to the `ktpass` service, do not make changes to the user. For example, do not change the password. If you do change the user, the key version increases and you must update the **Version Key** in the **New Authentication Principal Properties** window in SmartEndpoint.

To prepare the Active Directory Server for authentication:

1. On the Active Directory Server, run the `ktpass.exe` in this folder:

   `C:\Windows\System32`

2. Go to **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

3. Create a domain user and clear the **User must change password at next logon** option.
4. Run this command to map a service to a user:

   Syntax:

   ```
   ktpass princ ServiceName/realm@REALM mapuser
   <userName>@REALM pass <userPass> out <name of outFile>
   ```

   Example:

   ```
   ktpass princ tst/nac1.com@NAC1.COM mapuser auth-
   user@NAC1.COM pass 123456 out outfile.keytab
   ```

   Explanations:

Syntax	Example value	Explanation
`ServiceName`	`tst`	Name of the service.
`realm`	`nac1.com`	Domain name of the Active Directory server. The first instance is in lower case. The second in upper case.
`<userName>`	`auth-user`	The Active Directory domain user.
`<userPass>`	`123456`	Password for user.
`<name of outFile>`	`outfile.keytab`	Name of the encrypted keytab file.

5. Save the console output to a text file. See the version number (`vno`) and encryption type (`etype`).

   Sample output:

   ```
   Targeting domain controller: nac1-dc.nac1.com
   Successfully mapped tst/nac1.com to auth-user.
   WARNING: pType and account type do not match. This might cause problems.
   Key created.
   Output keytab to outfile.log:
   Keytab version: 0x502
   keysize 74 tst/nac1.com@NAC1.COM ptype 0 (KRB5_NT_UNKNOWN) vno 7 etype 0x17 (RC4-HMAC) keylength 16
   (0x32ed87bdb5fdc5e9cba88547376818d4)
   ```

   Important - We recommend that you do not use DES-based encryption for the Active Directory Domain Controller server, as it is not secure. If you choose to use DES encryption and your environment has Windows 7 clients, see sk64300.

Notes -

- Make sure that the clock times on the Endpoint Security servers and the Kerberos server are less than 5 minutes apart. If difference in the clock times is more than 5 minutes, a runtime exception shows and Active Directory authentication fails. On Gaia, use NTP or a similar service.

Step 2 of 3: Configuring Authentication Settings

Configure the settings in SmartEndpoint for client to server authentication.

Important - Use the **Unauthenticated** mode only for evaluation purposes. Never use this mode for production environments. Configure the authentication settings before moving to production.

How the Authentication Settings are Used in Deployment Packages

When you configure client package profiles, you choose an authentication account. The SSO Configuration details are included in the client deployment package, allowing the server to authenticate the client.

To configure authentication settings:

1. In SmartEndpoint open **Manage** > **Endpoints Authentication Settings**.

   The **Authentication Settings Properties** window opens.

2. Click **Add**.

   The **New Authentication Principal Properties** window opens.

3. Enter the details from the output of `ktpass.exe` that you configured in *"Step 1 of 3: Configuring the Active Directory Server for Authentication" on page 209*:

Field	Description
Domain name	Active Directory domain name. For example: `nac1.com`
Principle Name	Authentication service name in the format: `ServiceName/realm@REALM` This value must match the name that was configured in Active Directory > **New Object**. For example: `tst/nac1.com@NAC1.COM`

Field	Description
Version Key	Enter the version number according to the Active Directory output in the `vno` field. For example: `7`
Encryption method	Select the encryption method according to the Active Directory output in the `etype` field. For example: `RC4-HMAC`
Password	Enter (and confirm) the password of the Active Directory Domain Admin user you created for Endpoint Security use. For example: `123456`

4. Click **OK**.
5. When you are ready to work in Strong Authentication mode, select **Work in authenticated mode** in the **Authentication Settings Properties** window.
6. Click **OK**.

Important - After turning on Strong Authentication, wait one minute before initiating any client operations.
It will take time for the clients and the Endpoint Security Management Server to synchronize. During this time, the environment will remain unauthenticated, and some operations will fail. The exact amount of time depends on the synchronization interval (see *"Active Directory Scanner" on page 124*).

Step 3 of 3: Save Changes

After you have finished configuring strong authentication for Active Directory, save your changes.

1. Go to the **Policy** tab of SmartEndpoint.
2. In the **Policy Toolbar**, click **Save**.

UPN Suffixes and Domain Names

The User Principal Name (UPN) is the username in "email format" for use in Windows Active Directory (AD). The user's personal username is separated from a domain name by the "`@`" sign.

UPN suffixes are part of AD logon names. For example, if the logon name is `administrator@ad.example.com`, the part of the name to the right of the ampersand is known as the UPN suffix. In this case `ad.example.com`

When you configure a new user account in AD, you are given the option to select a UPN suffix, which by default will be the DNS name for your AD domain. It can be useful to have a selection of UPN suffixes available. If your AD domain name is `ad.example.com`, it might be more convenient to assign users a UPN suffix of `example.com`. To make additional UPN suffixes available, you need to add them to AD.

Configuring Alternative Domain Names

When configuring Strong Authentication for Active Directory communication between the Endpoint Security client and the Endpoint Security Management Server, you can configure multiple UPN suffixes for the Active Directory domain name.

To Configure Additional UPN Suffixes for Active Directory Authentication

1. In SmartEndpoint open **Manage** > **Endpoints Authentication Settings**.

   The **Authentication Settings Properties** window opens.

2. Click **Add**.

   The **New Authentication Principal Properties** window opens.

3. In the **Domain name** field, enter the alternative Active Directory domain name. For example, if the previously configured domain name is `nac1.com` add an alternative domain name such as `ad.nac1.com`

4. Configure the other fields with the same values as the previously configured authentication settings:

   - **Principle Name**
   - **Version Key**
   - **Encryption Method**
   - **Password**

5. Click **OK**.

6. Save the changes. Go to the **Policy** tab of SmartEndpoint, and in the Policy Toolbar, click Save 

Troubleshooting Authentication in Server Logs

To troubleshoot problems related to Active Directory Authentication, use the Authentication log on the Endpoint Security Management Server or Endpoint Policy Server in the `$UEPMDIR/logs/Authentication.log` file.

To see full debugging information in the Authentication.log file on an Endpoint Security server:

1. On the Endpoint Security server, run:

   ```
   export TDERROR_ALL_KERBEROS_SERVER=5
   ```

2. Restart the Endpoint Security server. Run:

   ```
   uepm_stop ; uepm_start
   ```

Results in Authentication.log

- If the **Authentication.log** file on the server shows:

  ```
  ERROR: Config file contains no principals
  ```

  The database was cleaned or the process to include authentication in the client package was faulty. To fix:

  1. Repeat the process to configure Active Directory authentication (See *"Configuring Active Directory Authentication" on page 209*).
  2. Make a new client package.
  3. Restart the Endpoint Security server:

     ```
     reboot
     ```

- If the **Authentication.log** file on the server shows:

  ```
  Permission denied in replay cache code
  ```

  Restart the Endpoint Security server:

  ```
  reboot
  ```

- If the **Authentication.log** file on the server shows:

  ```
  Clock skew too great
  ```

  - Make sure that the Endpoint Security Management Server and all clients are synchronized with the Active Directory server.

- Make sure that in the Windows Date and Time Properties window, the **Automatically adjust clock for daylight saving changes** option has the same value (selected or cleared) for all computers in the system, including the Active Directory server.
- The following workaround is not recommended, for security reasons, but is offered if you cannot fix the clock skew error with synchronization changes.

  To ensure that authentication occurs even if the clocks of the client, the Endpoint Security Management Server and the Active Directory server are out of synch, define an acceptable skew. By default, the authentication clock skew is 3600 seconds. You can change the Endpoint Security settings. In the `$UEPMDIR/engine/conf/global.properties` file, add this line: `authentication.clockSkew.secs=<seconds>`, where you replace `<seconds>` with the clock skew in seconds that you want to allow.

- If the **Authentication.log** file on the server shows:

  ```
  Key version number for principal in key table is incorrect
  ```

  Update the **Key version number** in the **Active Directory SSO Configuration** window.

  You might have changed the user that is mapped to the `ktpass` service (see *"Step 1 of 3: Configuring the Active Directory Server for Authentication" on page 209*.

To turn off full debugging information on the Endpoint Security server:

1. On the Endpoint Security server, unset the debug variable:

   ```
   unset TDERROR_ALL_KERBEROS_SERVER
   ```

2. Make sure that the output is empty:

   ```
   echo $TDERROR_ALL_KERBEROS_SERVER
   ```

3. Restart the Endpoint Security server. Run:

   ```
   uepm_stop ; uepm_start
   ```

Troubleshooting Authentication in Client Logs

The Authentication.log file for each Endpoint Security client is on the client computer at `%DADIR%/logs`.

A normal log is:

```
[KERBEROS_CLIENT(KerberosLogger_Events)] : Credentials acquired
for John@ACME-DOM.COM
[KERBEROS_MESSAGE(KerberosLogger_Events)] : Message is Empty.
[KERBEROS_CLIENT(KerberosLogger_Events)] : Security context is not
yet established.continue needed.
```

If the **Authentication.log** file on the client shows:

```
No authority could be contacted for authentication.
```

The Endpoint Agent cannot find a Domain Controller to supply credentials.

To fix this:

1. Make sure that the client is in the domain and has connectivity to your Domain Controller.
2. To authenticate with user credentials, log off and then log in again.

   To authenticate with device credentials, restart the computer.

If the **Authentication.log** file on the client shows:

```
The specified target is unknown or unreachable
```

Check the service name. Make sure that there are no typing errors and that the format is correct.

If there was an error, correct it on the Check Point Endpoint Security Management Server.

Full Disk Encryption

Full Disk Encryption gives you the highest level of data security for Endpoint Security client computers. It combines boot protection and strong disk encryption to ensure that only authorized users can access data stored in desktop and laptop PCs.

When configuring the Full Disk Encryption policy, you choose an encryption engine for groups of computers. The encryption engine can be either *"Check Point Full Disk Encryption" below* or *"BitLocker Encryption for Windows Clients" on page 240*.

Check Point Full Disk Encryption

Check Point Full Disk Encryption has two main components:

- **Disk encryption** ensures that all volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files. There is no user downtime because encryption occurs in the background without noticeable performance loss. The encrypted disk is inaccessible to all unauthorized people.
- **Pre-boot Protection** requires users to authenticate to their computers before the computer boots. This prevents unauthorized access to the operating system using authentication bypass tools at the operating system level or alternative boot media to bypass boot protection.

Configure the settings for Check Point Full Disk Encryption in SmartEndpoint in the **Policy** tab > **Full Disk Encryption** rules.

Configuring a Check Point Full Disk Encryption Policy

You can use the default Full Disk Encryption rule **Default Full Disk Encryption settings for the entire organization**. Edit the actions of the rule to your requirements. and install the policy.

Alternatively, use the following procedure to create a new Check Point Full Disk Encryption policy rule and configure actions for a specific organizational unit. After you install the Full Disk Encryption policy, make sure the policy is installed on the client.

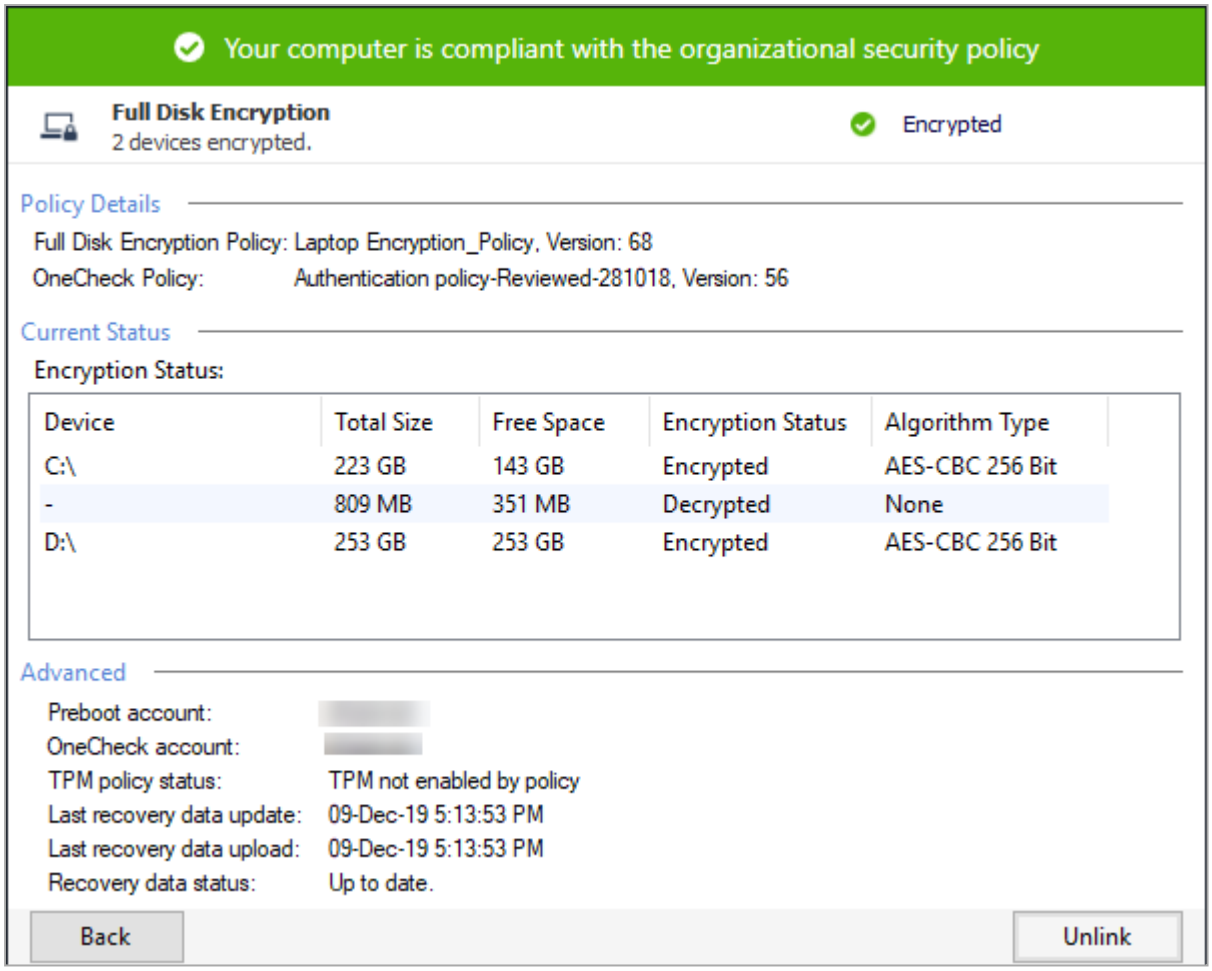
Configuring the Check Point Full Disk Encryption policy for a specific organizational unit

1. Open SmartEndpoint and go to the **Policy** tab.
2. In the Policy toolbar, click the **Create a Rule** button .

   The **Create Rule Wizard** opens.
3. Select **Full Disk Encryption**
4. Click **Next**.
5. In the **Select Entities page**, select the computers for which you want to configure Check Point Full Disk Encryption.
6. Click **Next**.
7. In the **Change rule action settings** page, select **Encryption Engine: Use Check Point Full Disk Encryption** .
8. Optionally, make changes to the default action settings.
9. Click **Next**.
10. In the **Enter rule name and comment** page, fill in the details.
11. Click **Finish**.
12. In the main toolbar, click **Save rule**, and **Install the Policy**.

Making sure the Full Disk Encryption policy is installed on the client

1. On the Windows client computer, in the system tray, right-click the lock icon of the Endpoint Security client.
2. Select **Display Overview** and open the **Full Disk Encryption** page.
3. Make sure the **Policy Details** show the Full Disk Encryption Policy.


Your computer is compliant with the organizational security policy
Full Disk Encryption
2 devices encrypted.
Encrypted
Policy Details
Full Disk Encryption Policy: Laptop Encryption_Policy, Version: 68
OneCheck Policy: Authentication policy-Reviewed-281018, Version: 56
Current Status
Encryption Status:
Device
Total Size
Free Space
Encryption Status
Algorithm Type
C:\
223 GB
143 GB
Encrypted
AES-CBC 256 Bit
-
809 MB
351 MB
Decrypted
None
D:\
253 GB
253 GB
Encrypted
AES-CBC 256 Bit
Advanced
Preboot account:
OneCheck account:
TPM policy status:
TPM not enabled by policy
Last recovery data update:
09-Dec-19 5:13:53 PM
Last recovery data upload:
09-Dec-19 5:13:53 PM
Recovery data status:
Up to date.
Back
Unlink

Volume Encryption

These actions define if the volumes of the hard disk are encrypted or not.

Action	Description
Encrypt all local hard disks	All volumes of the hard disk are automatically fully encrypted. The encrypted disk is only accessible to authorized users.
Do not encrypt local hard disks - Encrypt only minimum volumes required for Pre-boot	The hard disk is not encrypted.

Double-click an action to edit the properties.

- **Volume encryption algorithm**: Full Disk Encryption can use these encryption algorithms:
  - XTS-AES (256-bit)
  - XTS-AES (128-bit)
  - AES-CBC (256-bit) - Default
  - Blowfish (256-bit)
  - Cast (128-bit)
  - 3DES (168-bit)
- **What is encrypted:** By default all drives that are detected after the installation and all visible disk volumes are encrypted. IRRT devices are not encrypted.

To change the volumes and devices that are encrypted, select these options:

- To have only minimum encryption for Pre-boot protection, select **Minimum volumes for Pre-boot authentication**.
- To select the exact drives that are encrypted, select **Custom Volume Encryption** and click **Configure Volumes**.
- To encrypt volumes that are found after the initial Full Disk Encryption installation on a computer, select **Allow encryption of volumes that were detected after the initial installation**.
- To encrypt IRRT devices, select **Allow protection/encryption on IRRT devices**.
- To use a Self-Encrypting drive (SED), select **Allow using the hardware encryption functionality of self-encrypting drives**.

  Self-Encrypting drives encrypt and decrypt immediately.

Custom Disk Encryption Settings

If you select **Custom Volume Encryption** for the **Encrypted disks and volumes** setting, configure the encryption and Pre-boot settings for each volume.

To configure the settings for each volume:

1. In the **Custom Volume Encryption Settings** window, click **Add**.
2. Select the disk number and volume number to configure.
3. To enable Pre-boot on the volume, select **Pre-boot**.
4. To encrypt the volume, click **Encrypt**.
5. Click **OK**.

Self-Encrypting Drives

To configure volume encryption settings for Self-Encrypting drives, edit the **Volume Encryption** action of the Full Disk Encryption rule.

The disk encryption setting **Allow Self-Encrypting Drives (SED) hardware functionality** lets Full Disk Encryption probe and use SED disks that comply with the OPAL standard. If a compatible system and disk are detected, Full Disk Encryption uses the hardware encryption on the disk instead of the traditional software encryption.

When using SED drives, do not change the default settings for **Encrypted disks and volumes**. The required settings are:

- **Encrypt all visible disk volumes**
  - **Boot protect hidden disk volumes**
    - **Encrypt hidden disk volumes**

When SED encryption is in effect on a client computer, the **Drive Information** in the **Encryption Status** of the client shows SED added to the volume name. You can see this in the Client UI and in the **Computer Details** > **Full Disk Encryption** in SmartEndpoint.

- AES encryption is always used with SED drives.
- You cannot use custom volume encryption with SED drives. The client overrides custom volume configuration.
- Manage SED drives in the same way as software-encrypted drives.

For SED Requirements, see the Release Notes for your Endpoint Security client version. Either search the Web for the release notes, or:

1. Open the *Endpoint Security Homepage* .
2. Go to **Detailed Information per Release** > **Detailed Client Releases Information**.

3. Find the row for your client version.
4. In the **Additional information** column, click **Documentation**.
5. Click the link to the Release Notes.

Authentication before the Operating System Loads (Pre-boot)

The **Pre-boot Protection** action of a Full Disk Encryption rule defines if users must authenticate in the Pre-boot before the operating system loads. Configure the Pre-boot authentication method and other settings related to user authentication in the OneCheck User Settings rules.

Note - Password Synchronization only works if Pre-boot authentication is enabled.

Action	Description
Authenticate user before OS loads (Pre-boot)	Users must authenticate to their computers in the Pre-boot before the operating system loads.
Do not authenticate user before OS loads (Not recommended)	This setting disables pre-boot, and is not recommended. This option allows the user to bypass the Pre-boot authentication at the cost of reducing the security of the solution to a level below encryption strength. Consider using SSO or enable bypass Pre-boot when connected to LAN. Users authenticate to their computers only at the operating system level. **Note**: To reduce security issues, configure settings in **Require Pre-boot if one or more of these conditions are met**.

Double-click an action to edit the properties.

If you choose **Authenticate user before OS loads (Pre-boot)**, you can choose **Temporary Pre-boot bypass (Wake on LAN) settings** to bypass Pre-boot in specified situations:

- **Allow bypass when connected to LAN** - On computers that are connected to an Endpoint Security server through Ethernet, Pre-boot is not necessary. The client automatically authenticates securely through the network without Pre-boot. If automatic network authentication is not possible, manual Pre-boot authentication is required. This option is supported on UEFI and Mac computers. See *Unlock on LAN Requirements* in the Release Notes for your Endpoint Security client version. Either search the Web for the Release Notes, or find them in the *Endpoint Security Homepage*.
  - **Unlock Pre-boot user on successful OS login** - If users are away from the LAN and get locked out of Pre-boot (because of incorrect logons), they can log on the next time they are on the LAN. When they log on to the operating system, the Pre-boot lock is unlocked.
- **Allow OS login after temporary bypass** - For scenarios when you want to temporarily bypass the Pre-boot, for example, for maintenance, see *"Temporary Pre-boot Bypass" on the next page*. Temporary Pre-boot Bypass reduces security.

If you choose **Do not authenticate user before OS loads (Not recommended)**, the user experience is simpler, but it is less secure. Users log in to Windows only, and the options in **Integrate with OS login** part of the action properties become available. To reduce security issues, configure settings in **Require Pre-boot if one or more of these conditions are met**:

- Single Sign-On (SSO) together with Pre-boot Authentication.
- Pre-boot with **Bypass Pre-boot when connected to LAN**.
- **Display Last Logged on User in Pre-boot** - The username of the last logged on user shows in the Pre-boot logon window. That user only needs to enter a password or Smart Card pin to log in.
- **Use TPM for Pre-boot integrity** -This uses the TPM security chip to measure Pre-boot components. If they are not tampered with, the TPM allows the system to boot. See sk102009 for more details.

  Note: The software based hardware hash is disabled when TPM is configured.

  You can also use TPM in addition to Pre-boot authentication for two-factor authentication.

Temporary Pre-boot Bypass

Temporary Pre-boot Bypass lets the administrator disable Pre-boot protection temporarily, for example, for maintenance. It was previously called Wake on LAN (WOL).

You enable and disable Temporary Pre-boot Bypass for a computer, group, or OU from the computer or group object. The Pre-boot settings in the Full Disk Encryption policy set how Temporary Pre-boot Bypass behaves when you enable it for a computer.

Temporary Pre-boot Bypass reduces security. Therefore use it only when necessary and for the amount of time that is necessary. The settings in the Full Disk Encryption policy set when the Temporary Pre-boot Bypass turns off automatically and Pre-boot protection is enabled again.

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

- Temporary Pre-boot Bypass
- Temporary Pre-boot Bypass from a script
- Temporary Pre-boot Bypass when connected to LAN

To temporarily disable Pre-boot on a computer:

1. In the Computer Details or Node Details window, select **Security Blades** > **Full Disk Encryption**. Or, right-click a node and select **Full Disk Encryption** > **Disable Pre-boot Protection**.

2. Click **Temporarily Disable Pre-boot**.
3. Click **Yes**.

The Pre-boot is enabled again when you click **Revert to Policy Configuration** or when the criteria in the Temporary Pre-boot Bypass settings are met.

To configure Temporary Pre-boot Bypass settings:

1. In a **Full Disk Encryption** rule in the **Policy**, right-click the **Authenticate before OS loads Pre-boot** Action and select **Edit Shared Action**.
2. Click **Temporary Pre-boot Bypass (Wake on LAN) settings**.
3. Select the type of Temporary Pre-boot Bypass to allow:
   - **Allow Temporary Pre-boot Bypass (Wake On LAN)**
   - **Allow bypass script**. Also see *"Temporary Pre-boot Bypass with a Script" on the next page*.
   - **Allow bypass when connected to LAN**
4. Click the link next to the option to configure when the selected type of Temporary Pre-boot Bypass occurs: **By Demand**, **Once**, or **Weekly**.
5. Select the date and time.
6. In **Temporary Pre-boot Bypass duration**, select when Temporary Pre-boot Bypass functionality become disabled. You must select 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 or hours** -Select this to turn off the bypass after the configured amount of time passed.

   After the number automatic logons occur or the number of days or hours expires, Temporary Pre-boot Bypass is disabled on the client and the Pre-boot environment shows. Select a small number so that you do not lower the security by disabling the Pre-boot for a long time.
7. Click **OK**.

Note - If the mouse is moved or a key pushed on the keyboard in the Pre-boot environment, the Temporary Pre-boot Bypass functionality is disabled.

Temporary Pre-boot Bypass with a Script

If you run scripts to do unattended maintenance or installations (for example, SCCM) you might want the script to reboot the system and let the script continue after reboot. This requires the script to turn off Pre-boot when the computer is rebooted. Enable this feature in the **Temporary Pre-boot Bypass Settings** windows. The Temporary Pre-boot Bypass script can only run during the timeframe configured in **Temporary Pre-boot Bypass Settings**.

Running a Temporary Pre-boot Bypass script

In a script you execute the **FdeControl.exe** utility to enable or disable Pre-boot at the next restart:

- Run: `FDEControl.exe set-wol-on` to enable Temporary Pre-boot Bypass.
- Run: `FDEControl.exe set-wol-off` to disable Temporary Pre-boot Bypass.

The above commands will fail with code 13 (UNAUTHORIZED) if executed outside the timeframe specified in the policy.

Temporarily Require Pre-boot

If you do not require Pre-boot, users go straight to the Windows login. Because this makes the computer less secure, we recommend that you require Pre-boot authentication in some scenarios.

To temporarily require Pre-boot:

1. In a **Full Disk Encryption** rule in the **Policy**, right-click the **Do not authenticate before OS loads Pre-boot** Action and select **Edit Properties**.
2. Configure these options to **Require Pre-boot authentication if one or more of these conditions are met**:
    - **More than X failed logon attempts were made** - If a user's failed logon attempts exceed the number of tries specified, Pre-boot is required. The computer automatically reboots and the user must authenticate in Pre-boot.
    - **The hard disk is not used by the original computer (hardware Hash)** -If selected, the client generates a hardware hash from identification data found in the BIOS and on the CPU. If the hard drive is stolen and put in a different computer, the hash will be incorrect and Pre-boot is required. The computer reboots automatically, and the user must authenticate in Pre-boot.

      Warning - Clear this option before you upgrade BIOS firmware or replace hardware. After the upgrade, the hardware hash is automatically updated to match the new configuration.

- **The computer cannot reach any of the configured locations** - Requires Pre-boot when Location Awareness requirements are not filled. If you select this, configure the locations that the computer tries to reach in the list below.

3. **Before Pre-boot authentication is required, show this message** -Enter a message to display to the user if a configured condition is met and Pre-boot is required. For example, to call the Help Desk if the Pre-boot window opens.
4. Click **Use TPM for Pre-boot integrity** to use the TPM security chip available on many PCs during pre-boot in conjunction with password authentication or Dynamic Token authentication. The TPM measures Pre-boot components and combines this with the configured authentication method to decrypt the disks. If Pre-boot components are not tampered with, the TPM lets the system boot. See sk102009 for more details.

Advanced Pre-boot Settings

You can set these Pre-boot Environment Permissions in the properties of the Pre-boot Protection action in a Full Disk Encryption policy rule. The hardware related setting are only for systems with BIOS firmware and do not affect systems with UEFI.

Note - These permissions are also in the Pre-boot Customization Menu on client computers. To open the Pre-boot Customization Menu:

- **On BIOS systems** - Press both shift keys on a client computer while Full Disk Encryption loads during the start up.
- **On UEFI systems** - Press the Ctrl and Space key on the computer keyboard.

Permission	Notes
Enable USB device in Pre-boot environment (BIOS only)	Select to use a device that connects to a USB port. If you use a USB Smart Card you must have this enabled. If you do not use USB Smart Cards, you might need this enabled to use a mouse and keyboard during Pre-boot.
Enable PCMCIA (BIOS only)	Enables the PCMCIA Smart Card reader. If you use Smart Cards that require this, make sure it is enabled.
Enable mouse in Pre-boot environment (BIOS only)	Lets you use a mouse in the Pre-boot environment.
Allow low graphics mode in Pre-boot environment (BIOS only)	Select to display the Pre-boot environment in low-graphics mode.

Permission	Notes
Maximum number of failed logons allowed before reboot	■ If active, specify the maximum number of failed logons allowed before a reboot takes place. ■ This setting does not apply to smart cards. Smartcards have their own thresholds for failed logons.
Verification text for a successful logon will be displayed for	Select to notify the user that the logon has been successful, halting the boot-up process of the computer for the number of seconds that you specify in the Seconds field.
Allow hibernation and crash dumps	Select to allow the client to be put into hibernation and to write memory dumps. This enables Full Disk Encryption protection when the computer is in hibernation mode. **Note:** hibernation must be enabled in Windows for this option to apply. All volumes marked for encryption must be encrypted before Full Disk Encryption permits the computer to hibernate.
Enable TPM two factor authentication (Password & Dynamic Tokens)	Select to use the TPM security chip available on many PCs during pre-boot in conjunction with password authentication or Dynamic Token authentication. The TPM measures Pre-boot components and combines this with the configured authentication method to decrypt the disks. If Pre-boot components are not tampered with, the TPM lets the system boot. See sk102009 for more details.
Firmware update friendly TPM measurements	Disables TPM measurements on Firmware/BIOS level components. This makes updates of these components easier but reduces the security gained by the TPM measurements because not all components used in the boot sequence are measured. If this setting is enabled on UEFI computers, the Secure Boot setting is included in the measurement instead of the firmware.
Enable Remote Help	Select to let users use Remote Help to get users access to their Full Disk Encryption protected computers if they are locked out.
Remote Help response length	Configure how many characters are in the Remote Help response that users must enter.

User Authorization before Encryption

Full Disk Encryption policy settings enable user acquisition by default. If user acquisition is disabled, the administrator must assign at least one Pre-boot user account to each client computer before encryption can start.

You can require one or more users to be acquired before encryption can start.

You can also configure clients to continue user acquisition after Pre-boot is already enabled. This might be useful if a client computer is used by many users, also called roaming profiles.

Action	Description
Automatically learn and authorize logged in users	Before hard disk encryption, automatically register users that access their local computers and authorize them to access their computers after encryption. **Note** - It is always possible to manually authorize users to access encrypted computers
Manually authorize users to access encrypted computers	Administrators must manually authorize users to their computers after encryption.

Double-click an action to edit the properties.

Usually a computer has one user and only one user must be acquired. If the computer has multiple users, it is best if they all log on to the computer for Full Disk Encryption to collect their information and acquire them.

Before you enable **Automatically learn and authorize logged in users**, make sure clients can get device and user policies from the server.

To configure settings for Automatically learn and authorize logged in users:

- **Pre-boot enforcement will begin after** - Endpoint Security can start to enforce Pre-boot for acquired users before user acquisition is completed. Select when this starts:
  - **The acquisition process has acquired x user(s)** - Select how many users to acquire before Pre-boot becomes enforced on acquired users.

    If you enter **3**, encryption does not start until three users log on to the computer.

- **At least one user has been acquired after x day(s)** - Select how long to wait before Pre-boot is enforced on acquired users.

  This setting limits the number of days when user acquisition is active for the client. If the limit expires and one user is acquired, Pre-boot is enforced and encryption can start. If no users are acquired, user acquisition continues.

  Pre-boot becomes enforced on acquired users after one of the criteria are met.

- **Continue to acquire users after Pre-boot has been enforced** - Pre-boot is active for users who were acquired and user acquisition continues for those who were not acquired.

  - **User acquisition will stop after having acquired additional (x) user(s)** - User acquisition continues until after the selected number of additional users are acquired.

Note - If you need to terminate the acquisition process, for example the client fails to acquire users even though an unlimited time period is set, define a new policy where automatic acquisition is disabled.

Single Sign-On With OneCheck Logon

OneCheck Logon is a Single Sign-On solution that let users log at one time to authenticate to all these :

- Full Disk Encryption
- DLP
- Windows
- VPN

When OneCheck Logon is enabled, a different logon window opens that looks almost the same as the regular Windows authentication window. The logon credentials are securely stored internally.

These actions define if you enable OneCheck Logon:

Action	Description
Enable lock screen authentication (OneCheck) Enable OneCheck Identity Single Sign On for OS	Users log on one time to authenticate to the operating system, Full Disk Encryption, and other Endpoint Security components.
Use native sign on for OS	Use the native OS logon mechanism. You can enable Single-Sign On (not OneCheck) in OneCheck User Settings to have one log on that applies to the OS and Full Disk Encryption.

Double-click an action to edit the Properties.

To configure OneCheck Logon properties:

1. Select **Enable lock screen authentication (OneCheck)**.
2. Optional: Configure the Check Point Endpoint Security screensaver.
    - The screensaver is active only after a Full Disk Encryption policy has been installed on the client.

- After selecting the Check Point Endpoint Security screensaver option, enter the:
  - Text that shows when the screensaver is active.
  - Number of minutes the client remains idle before the screensaver activates.

3. Optional: Select **Require that only an authorized Pre-boot user is allowed to log into Windows**. If selected, only users that have permission to authenticate to the Pre-boot on that computer can log on to the operating system.
4. Optional: Select **Use Pre-boot account credentials in OS lock screen**. If selected, users authenticate in the regular Operating System login screen but with the credentials configured for Pre-boot.

   Best practice is to only use this feature when there is no Active Directory available. For customers that use Active Directory, we recommend a combination of User Acquisition, OneCheck Logon, and Password Synchronization that will let users use the same credentials for Pre-boot and Windows login.

Check Point Full Disk Encryption Recovery

If system failure prevents the operating system from starting on a client computer, Check Point Full Disk Encryption has these options:

Full Recovery with Recovery Media - Decrypts the failed disk. This takes more time than Full Disk Encryption Drive Slaving Utility and Dynamic Mount Utility that let you access data quickly.

If system failure prevents the operating system from starting on a client computer, you can use **Full Disk Encryption Recovery Media** to decrypt the computer and recover the data. Client computers send recovery files to the Endpoint Security Management Server one time during the initial deployment so that you can create recovery media if necessary. After the recovery, the files are restored as decrypted, like they were before the Full Disk Encryption installation, and the operating system can run without the Pre-boot.

After the recovery, you must install Full Disk Encryption on the computer.

Recovery Media:

- Is a snapshot of a subset of the Full Disk Encryption database on the client.
- Contains only the data required to do the recovery.
- Updates if more volumes are encrypted or decrypted.
- Removes only encryption from the disk and boot protection.
- Does not remove Windows components.
- Restores the original boot record.

Users must authenticate to the recovery media with a username and password. There are the options for which credentials to use:

- Users that are assigned to the computer and have the **Allow use of recovery media** permission (in **OneCheck User Settings rule** > **Advanced** > **Default logon settings)** can authenticate with their regular username and password.
- When you create the recovery media, you can create a temporary user who can authenticate to it. A user who has the credentials can authenticate to that recovery media. Users do not require **Allow use of recovery media** permission to use the recovery media. Smart Card users must use this option for recovery.

Creating Data Recovery Media

You can create Full Disk Encryption recovery media that can run on a failed computer to decrypt it. Create the recovery media on the server or with an external tool.

The media can be on a CD/DVD, USB device, or REC file.

Note - Creating a recovery media on a USB flash disk formats the device and removes all previous content.

To create recovery media from the Endpoint Security Management Server:

1. In Smart **Endpoint**, select **Tools** > **Encryption Recovery Media**.

   The **Full Disk Encryption Recovery Media Tool** window opens.

2. Double-click a folder from the navigation tree to see the users and computers that it contains.

3. Right-click the computer to restore and then select **Encryption Recovery Media**.

   The target retrieves the last known recovery data that was uploaded to the server by the client.

4. Users who have permission to use recovery media for the computer show in the **Users Allowed to Recover** area.

   - If the user who will do the recovery shows on the list, continue to the next step.
   - If the user who will do the recovery is not on the list:

     a. Click **Add** to create a temporary user who can use the recovery media.

     b. In the window that opens add a username and password that the user will use to access the file.

5. Select a destination for the Recovery Media:

   - For a bootable CD/DVD, enter a path to a directory for the ISO file
   - For an REC file, enter a path to a directory for the file.
   - For a USB device, select the target drive from the list.

6. Click **Write Media**.

7. Give the Recovery Media file or device to the user who will do the recovery.

8. Make sure the user knows:

   - Which username and password to use.
   - How to boot the computer: with a CD or USB device.

To create recovery media using the external recovery media tool:

1. On an Endpoint Security client, go to folder: `C:\Program Files (x86)\CheckPoint\Endpoint Security\Full Disk Encryption\`

2. Double-click `UseRec.exe` to start the external recovery media tool.

3. Follow directions in the tool to create recovery media.

Using Data Recovery Media

Use the newly created Full Disk Encryption recovery media to decrypt the failed computer.

To recover an encrypted computer:

1. On the failed computer, run the recovery media from a CD/DVD or bootable USB device.
2. When the **Recovery Console Login** windows shows, enter the name and password of a user on the recovery media.

   The disk decrypts using partition keys contained in the Recovery Media.

   Note - During the decryption process, the client cannot run other programs.

Full Disk Encryption Drive Slaving Utility - Use this to access specified files and folders on the failed, encrypted disk that is connected from a different "host" system.

Full Disk Encryption Drive Slaving Utility lets you access Full Disk Encryption protected disk drives that become corrupted as a result of an Operating System failure . The Drive Slaving Utility is hardware independent.

Full Disk Encryption Dive Slaving Utility replaces older versions of Full Disk Encryption drive slaving functionality, and supports R73 and all E80.x versions. You can use the Full Disk Encryption Drive Slaving Utility instead of disk recovery.

Notes -

- On an E80.x client computer with 2 hard disk drives, the Full Disk Encryption database can be on a second drive. In this case, you must have a recovery file to unlock the drive without the database.
- Remote Help is available only for hard disk authentication. It is not available for recovery file authentication.

Before You Use the Drive Slaving Utility

Before you run the Full Disk Encryption Drive Slaving Utility, make sure to do these:

- Authenticate the Full Disk Encryption encrypted disk
- On systems with active Pre-boot Bypass, you must authenticate with Full Disk Encryption account credentials

We recommend that you use a recovery file when you are not sure if the hard disk drive or the Full Disk Encryption internal database on your system are corrupted.

Using the Drive Slaving Utility

To use the Full Disk Encryption Drive Slaving Utility:

1. On a computer with Check Point Full Disk Encryption installed, run this command to start the Full Disk Encryption Drive Slaving Utility: `<x:>\Program files (x86)\CheckPoint\Endpoint Security\Full Disk Encryption\fde_drive_slaving.exe`

   Note - To unlock a protected USB connected hard disk drive, you must first start the Drive Slaving Utility, and then connect the disk drive.

   The Full Disk Encryption - Drive Slaving window opens.

2. Select a Full Disk Encryption protected disk to unlock.

   Unlock volume(s) authentication window opens.

3. Enter **User account name** and **Password**.

4. Click **OK**.

After successful authentication, use Windows explorer to access the disk drive. If you fail to access the locked disk drive, use the Full Disk Encryption Recovery file, then run the Drive Slaving Utility again.

Note - To prevent data corruption, shut down the system or use a safe removal utility before you disconnect the USB connected drive.

Dynamic Mount Utility - Use this to access specified files and folders on the failed, encrypted disk. You create a WinPE CD/DVD media that contains the Dynamic Mount Utility application. Boot the WinPE CD/DVD media on the failed, encrypted computer. When users authenticate through the Dynamic Mount Utility they can extract files and folders from the encrypted system.

To access data on the hard disk of a Full Disk Encryption-protected computer without doing a Recovery, use the Dynamic Mount Utility of Full Disk Encryption. See sk108858.

Check Point Full Disk Encryption Self-Help Portal

The Self-Help Portal lets users reset their own passwords for Full Disk Encryption. 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 Self-Help Portal only works with Active Directory users. Make sure that the Endpoint Security Active Directory Scanner is configured and that the Active Directory is scanned.

The portal is available for desktop and mobile devices.

For supported browsers and devices, see the .

Activating the Self-Help Portal

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

Note - In **Gaia Portal > Hosts and DNS** page, make sure to configure:

- The DNS Sever
- Domain Name
- DNS suffix

To enable the Self-Help Portal:

On the Endpoint Security Management Server, run these commands:

```
cd $UEPMDIR/engine/scripts
```

```
selfhelp_cmd enable
```

Note that this restarts the Endpoint Security Management Server.

After activation, the Self-Help Portal is available at:

```
http://<IP Address of Endpoint Security Management Server>/eps_shp
```

To disable the Self-Help Portal, run:

```
selfhelp_cmd disable
```

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

```
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 **OneCheck User Settings** 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 **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://<IP Address of Endpoint Security Management Server>/eps_shp`

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 (OneCheck)**.
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.

3. A confirmation message shows. Click **Yes**.

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**.

BitLocker Encryption for Windows Clients

BitLocker lets you encrypt the hard drives on a Windows computer, and is an integral part of Windows. Check Point BitLocker uses the Endpoint Security Management Server, Client Agent and the SmartEndpoint UI to manage BitLocker. BitLocker Management is implemented as a Windows service component called Check Point BitLocker Management. It runs on the client together with the Client Agent (the Device Agent). Check Point BitLocker Management uses APIs provided by Microsoft Windows to control and manage BitLocker.

You can:

- Configure the BitLocker encryption policy. See *"Configuring a BitLocker Encryption Policy" on page 241*.
- Switch the encryption engine for selected clients from Check Point Full Disk Encryption to BitLocker Management, or from BitLocker Management to Full Disk Encryption. See *"Switching Between Check Point Full Disk Encryption and BitLocker Management" on page 244*.
- Take control of unmanaged computers so that they are centrally managed, either by Check Point BitLocker Management or by Check Point Full Disk Encryption. See *"Taking Control of Unmanaged BitLocker Computers" on page 246*.
- Recover data from a computer that is encrypted with BitLocker. See *"BitLocker Recovery" on page 247*.

Configure the settings for BitLocker in SmartEndpoint in the **Policy** tab > **Full Disk Encryption** rules.

Configuring a BitLocker Encryption Policy

To manage BitLocker encryption on Endpoint Security clients on Windows, configure the Full Disk Encryption Policy. You can use the default Full Disk Encryption rule **Default Full Disk Encryption settings for the entire organization**, change the action of the rule to **Use BitLocker Management**, and install the policy.

Alternatively, you can create a new rule and configure actions for a specific organizational unit.

Best Practices -

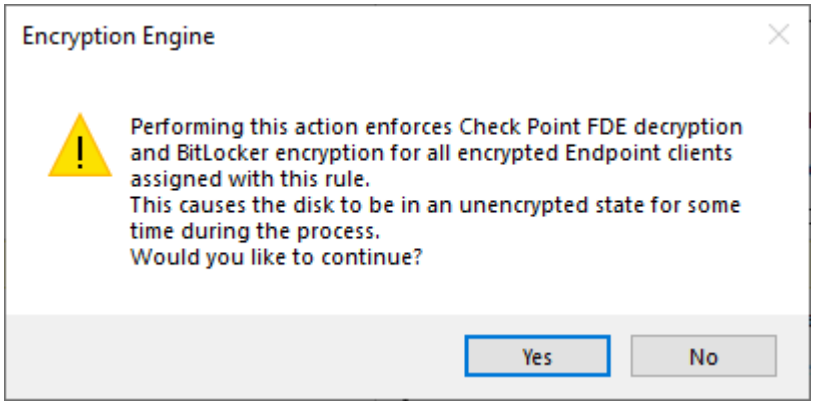
1. When you change the encryption policy for clients from Check Point Full Disk Encryption to BitLocker Management, the disk on the client is decrypted and then encrypted. This causes the disk to be in an unencrypted state for some time during the process. We recommend that you do not change the encryption policy for entire organization in one operation. Make the change for one group of users at a time.
2. Define the BitLocker policy before installing the Endpoint Security package on the client computers. This ensures that encryption will happen just one time, with BitLocker. It avoids Check Point FDE encryption followed by FDE decryption and BitLocker encryption.

Configuring the BitLocker encryption policy for a specific organizational unit

1. Open SmartEndpoint and go to the **Policy** tab.
2. In the toolbar of the Policy tab, click **Create a Rule** .

   The **Create Rule Wizard** opens.
3. Click **Full Disk Encryption**.
4. Click **Next**.
5. In the **Select Entities page**, select the computers for which you want to configure BitLocker encryption.
6. Click **Next**.
7. In the **Change rule action settings** page, click **Encryption Engine**, and select **Use BitLocker Management**.

   A warning message shows. Read it carefully.



8. Click **Yes**.

   Two actions remain: **Encryption Engine** and **Access Management**.

9. Edit the BitLocker Management policy: Click **Use BitLocker Management** and select **Edit Shared Action**.

10. Configure these settings:

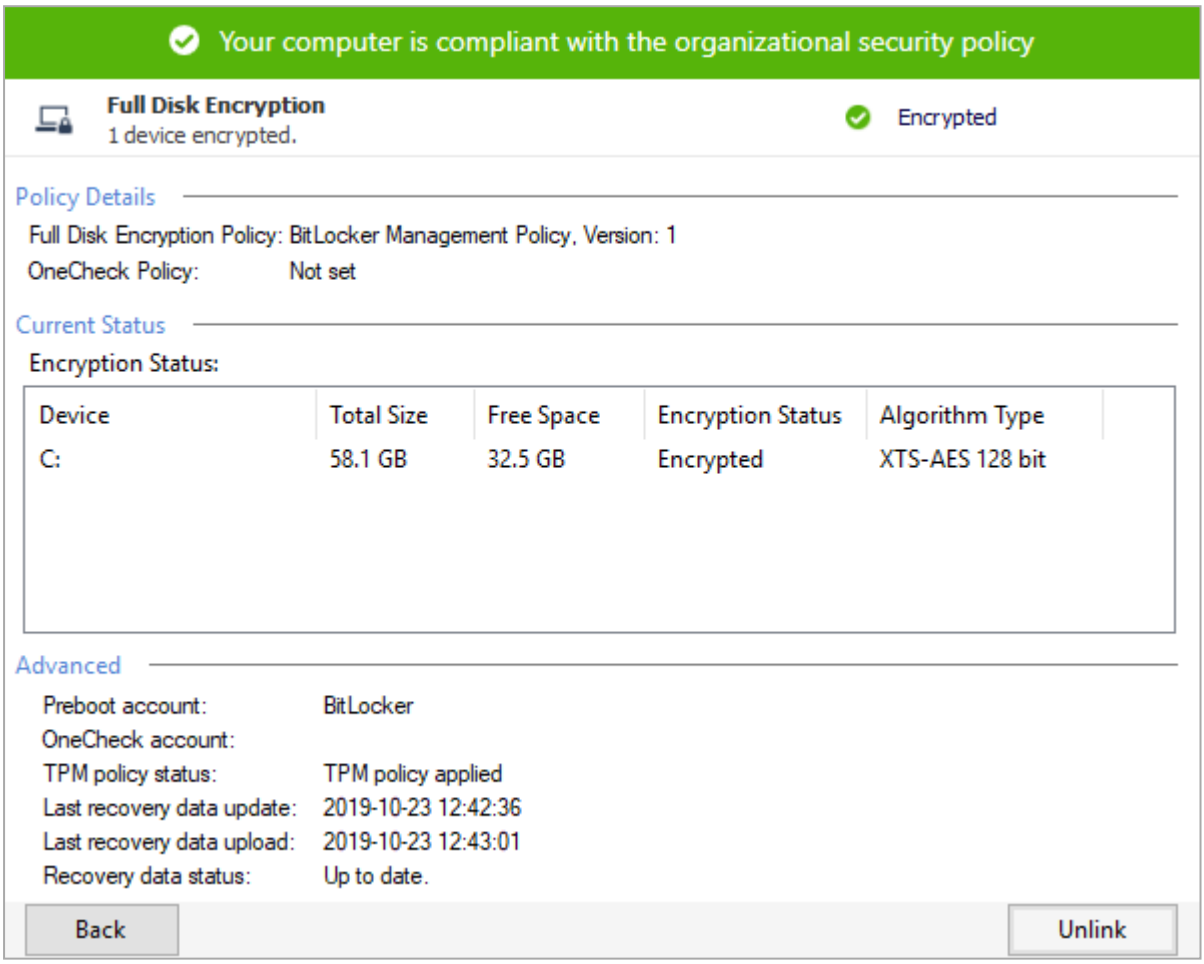
Setting	Options
Initial encryption type	■ *Encrypt entire drive* - Recommended for computers that are in production and already have user data, such as documents and emails. ■ *Encrypt used disk space only*, to encrypt only the data. Recommended for fresh Windows installations.
Drives to encrypt	■ *All drives* - Encrypt all drives and volumes. ■ *OS drive only* - Encrypt only the OS drive (usually C:\). This is the default.
Encryption algorithm	■ *Windows Default* - This is recommended. On Windows 10 Build 1507 or later, unencrypted disks are encrypted with XTS-AES-128. On encrypted disks, the encryption algorithm is not changed. ■ *XTS-AES-128* ■ *XTS-AES-256*

11. Click **OK**.
12. Click **Next**.
13. In the **Enter rule name and comment** page, fill in the details.
14. Click **Finish**.

15. In the main toolbar, click **Save rule**, and **Install the Policy**.

Making sure the BitLocker Management policy is installed on the Client

1. On the Windows client computer, in the system tray, right-click the lock icon of Endpoint Security client.
2. Select **Display Overview** and open the **Full Disk Encryption** page.
3. Make sure the **Policy Details** show the *BitLocker Management Policy*.



Switching Between Check Point Full Disk Encryption and BitLocker Management

You can switch the encryption engine for selected clients from Check Point Full Disk Encryption to BitLocker Management, or from BitLocker Management to Full Disk Encryption.

Best Practice - When you change the encryption engine of a client from Check Point Full Disk Encryption to BitLocker Management, or from BitLocker Management to Check Point Full Disk Encryption, the disk on the client is decrypted and then encrypted. This causes the disk to be in an unencrypted state for some time during the process. We recommend that you do not change the entire organization to BitLocker in one operation. Make the change for one group of users at a time.

Switching the encryption engine from Check Point Full Disk Encryption to BitLocker Management

1. Open SmartEndpoint and go to the **Policy** tab.
2. In the rule for Check Point Full Disk Encryption, in the **Actions** column, change the **Encryption Engine** action:

   From **Use Check Point Full Disk Encryption**

   To **Use BitLocker Management**.
3. In the main toolbar, click **Save rule**, and **Install the Policy**
4. On the *client computers* of the clients in the rule, this message shows:

5. The user must click **Reboot**.

   Decryption starts on the disk that is encrypted with Check Point Full Disk Encryption.

   When the decryption is complete, the message shows a second time on the client computer.
6. The user must click **Reboot**.

Encryption of the disk starts with BitLocker Management.

BitLocker Management with encryption is now active on the Endpoint Security client computers in the rule.

Switching the encryption engine from BitLocker Management to Check Point Full Disk Encryption

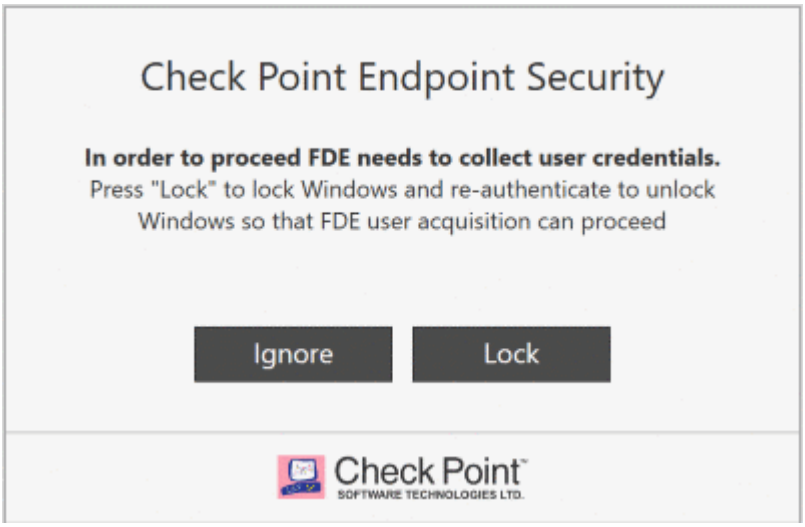
1. Open SmartEndpoint and go to the **Policy** tab.
2. In the rule for Check Point Full Disk Encryption, in the **Actions** column, change the **Encryption Engine** action:

   From **Use BitLocker Management**

   To **Use Check Point Full Disk Encryption**.
3. In the main toolbar, click **Save rule**, and **Install the Policy**.

   Decryption of the BitLocker managed disks starts on the Endpoint Security client computers in the rule.

   Encryption with Check Point Full Disk Encryption starts.
4. On the client computers this message shows:



5. To allow Full Disk Encryption to collect the credentials of the user, the user must click **Lock**.

Check Point Full Disk Encryption is now active on the Endpoint Security client computer in the rule.

Taking Control of Unmanaged BitLocker Computers

You can do a takeover of BitLocker-encrypted computers that are not managed by SmartEndpoint, and make them centrally managed. You can do this using either BitLocker Management or Check Point Full Disk Encryption.

Taking control of unmanaged BitLocker computers using BitLocker Management

Define and install a Full Disk Encryption policy with BitLocker Management. Follow the procedure in *"Configuring a BitLocker Encryption Policy" on page 241*, with these guidelines:

- Define a Full Disk Encryption rule that **Applies To** to either the **Entire Organization** or only to the entities that need BitLocker Management.
- In the properties of the **Use BitLocker Management** action, select **Windows Default** as the **Encryption algorithm**.

  This is important because it leaves the existing BitLocker encryption in place. Selecting another algorithm explicitly may result in a re-encryption if the existing algorithm does not match the algorithm in the policy. It is a good idea to avoid re-encryption because it can take a long time. The time it takes depends on the disk size, disk speed and PC hardware.

Taking control of unmanaged BitLocker computers using Check Point Full Disk Encryption

Follow the procedure for taking control of unmanaged BitLocker computers using BitLocker Management.

After the computers are under Check Point BitLocker Management, define a rule with Check Point Full Disk Encryption that **Applies To** to either the **Entire Organization** or only to the entities that need Check Point Full Disk Encryption. Follow the procedure in *"Configuring a Check Point Full Disk Encryption Policy" on page 218*.

Best Practice - When you change the encryption policy for clients from BitLocker Management to Check Point Full Disk Encryption, the disk on the client is decrypted and then encrypted. This causes the disk to be in an unencrypted state for some time during the process. We recommend that you do not change the encryption policy for entire organization in one operation. Make the change for one group of users at a time.

BitLocker Recovery

BitLocker recovery is the process by which you can restore access to a BitLocker-protected drive in the event that you cannot unlock the drive normally.

In SmartEndpoint you can use the *Recovery Key ID* for a computer to find the *Recovery Key* for an encrypted client computer. With the Recovery Key, the user can unlock encrypted drives and perform recoveries.

Important - Treat the Recovery Key like a password. Only share it using trusted and confirmed channels.

To get the Recovery Key for a client computer:

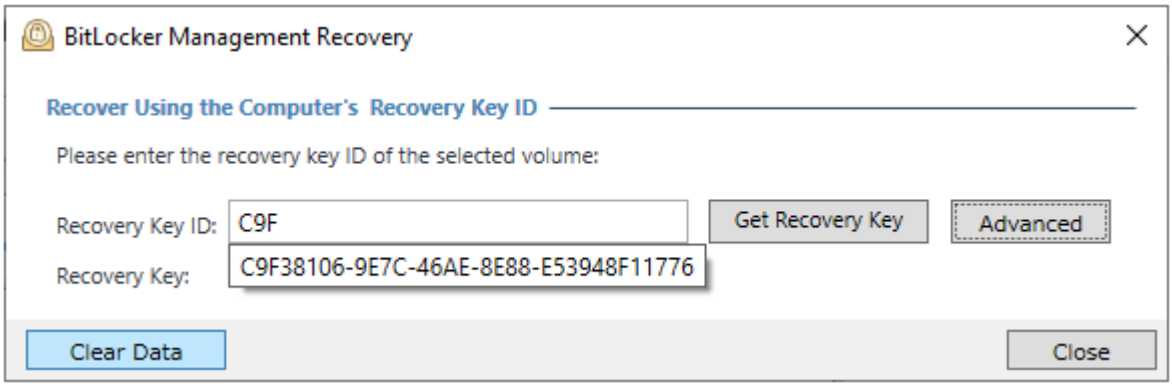
1. Open SmartEndpoint and go to **Menu** > **Tools** > **BitLocker Management Recovery**.

   The **BitLocker Management Recovery** window opens

2. Start typing the **Recovery Key ID** of the client. The Recovery Key ID is a string of numbers and letters that looks like this:

   C9F38106-9E7C-46AE-8E88-E53948F11776

   After you type a few characters, the Recovery Key ID fills automatically.



3. **Optional:** If you don't have the Recovery Key ID for the client, you can search for it. For this and other recovery options:

   a. Click **Advanced**.

      The **BitLocker Management Advanced Recovery** window opens.

   b. To search for the Recovery Key ID, type the **Common Name** of the computer, or browse for it

c. If the disk sectors containing the encrypted keys are damaged or unreadable, you can export to external media a BitLocker Key Package to use for recovery. In **Select File name and location**, browse to a location. To learn how to use the Microsoft recovery tools to decrypt the disk, see the Microsoft BitLocker Recovery Guide.

d. Click **Close**.

4. In the **BitLocker Management Recovery** window, click **Get Recovery Key**.

   The Recovery Key shows. It is a string of numbers that looks like this:

   409673-073722-568381-219307-302434-260909-651475-146696

5. On the client computer, type the Recovery Key.

Installing and Deploying Full Disk Encryption

After a package that includes Full Disk Encryption is successfully installed on a client, many requirements must be met before the Full Disk Encryption policy can be enforced. Before these requirements are met, the Pre-boot does not open. The period of time between the installation and when the policy can be enforced is called the Full Disk Encryption Deployment Phase.

To move from Deployment phase to Full Disk Encryption policy enforcement, these requirements must be met:

- There must be communication between the client and the server.
- The client must receive Full Disk Encryption and user policies from the server.
- Users must be acquired according to the configured policy.
- At least one user account must be configured.
- The client must send a recovery file to the server.
- The required System Area must be created and boot records must be updated according to the configuration (this includes the activation of Pre-boot).
- The device must have the Client requirements or Full Disk Encryption.

If there is communication between the client and server and the client meets the Client requirements, all of the requirements are completed automatically. However, if these requirements are not met, Full Disk Encryption cannot protect the computer and the Pre-boot cannot open.

Client Requirements for Full Disk Encryption Deployment

Note - Not all the Full Disk Encryption (FDE) requirements are shown here. For the complete FDE requirements, see the *Release Notes for your Endpoint Security client version*.

Clients must have:

- 32MB of continuous free space on the client's system volume

  Note - During deployment of the Full Disk Encryption component on the client, the Full Disk Encryption service automatically defragments the volume to create the 32MB of continuous free space, and suspends the Windows hibernation feature while the disk is encrypted.

Clients must **not** have:

- RAID.
- Partitions that are part of stripe or volume sets.

- Hybrid Drive or other similar Drive Cache Technologies. See sk107381.
- A compressed root directory. Subdirectories of the root directory can be compressed.

Other Requirements:

- All disks that are encrypted by FDE must have the same format (MBR or GPT)
- GPT-formatted disks are supported only on UEFI devices.
- Update the BIOS on the client computer to the latest version.
- If using the BIOS\UEFI option Fastboot, follow the precautions in sk140215.
- If using a third-party credential provider to log in to Windows, configure FDE to use (wrap) the third-party provider. See sk118817.

Completing Full Disk Encryption Deployment on a Client

For Check Point Full Disk Encryption, users are prompted to reboot their computers twice while Full Disk Encryption deploys. One time to make sure the Pre-boot is running before Full Disk Encryption encrypts the hard drive, and one time to validate the authentication credentials.

For BitLocker Encryption, users are prompted to reboot their computers once during the installation.

Stages of the Deployment Phase

You will see the status of the Deployment phase in:

- The Client Endpoint Security Main Page - In the Full Disk Encryption status.
- SmartEndpoint - In the **Computer Details** > **General Details**. Look at the **Blade Status** for Full Disk Encryption.
- The debug logs

These are the statuses as shown in the Client Endpoint Security Main Page:

- **Waiting for Policy** - Waiting for policy to be downloaded from server.
- **User Acquisition** - Users are acquired when they log on to Windows on the computer that has Full Disk Encryption installed. The number of users that must be acquired depends on the settings configured. Full Disk Encryption can become active after all users are acquired. User accounts must have passwords and fulfill password rules to be acquired.
- **Verifying Setup** - The client verifies that all of the settings are fulfilled properly and checks that users acquired are correct and fulfill password policies.

- **Deliver Recovery File** - The client sends a recovery file to the server. It includes users on the computer that have permission to use the recovery media.
- **Waiting for Restart** - The user must reboot the client. After it is rebooted, users will see the Pre-boot. Users get a message to log in with their Windows credentials. Then Full Disk Encryption starts to encrypt the volumes according to the policy.
- **Encryption in Progress** - Full Disk Encryption is encrypting the volumes.

Upgrading Full Disk Encryption

If you upgrade Endpoint Security from an earlier version of R80, R80.X, or E80.x, no special actions are required for Full Disk Encryption.

To upgrade Full Disk Encryption:

You must follow these procedures:

1. *"Upgrading Endpoint Security Clients" on page 153*
2. *sk99064 - How to upgrade Windows 8 to Windows 8.1 with Full Disk Encryption in place* .
3. *sk120667 - How to upgrade to Windows 10 1607 and above with Full Disk Encryption in-place* .

What effect does an upgrade have on users?

The upgrade does not have a significant effect on users.

Troubleshooting Full Disk Encryption

This section covers basic troubleshooting of Full Disk Encryption.

Using CPinfo

CPinfo is used to collect data about components in the Full Disk Encryption environment on the client. We recommend that you send the collected data to Check Point for analysis.

If you do not enter an output folder, CPinfo collects data about components in the Full Disk Encryption Pre-boot environment on the client.

Run CPinfo if:

- Encrypting or decrypting fails on Windows.
- The selected disk or volume does not encrypt or decrypt.
- Full Disk Encryption related issues occur.
- You experience system issues or crashes.

CPinfo gathers:

- All files in the data directory.
- Installation log.
- File version data for executables.
- Registry values for Full Disk Encryption
- GinaDll, UpperFilters and ProviderOrder.
- SMBios structure.
- Installed application lists.
- Microsoft Windows Partition list.

To run CPinfo:

1. In the notification area, right-click the client icon.
2. Select **Display Overview**.
3. In the right pane, click **Advanced**.
4. Click **Collect information for technical support**.

   CPinfo opens in the command prompt.
5. Press **ENTER** to start.

The information is collected. A window opens that shows the location of the cab file.

6. Press a key to exit CPinfo.

To Run CPinfo manually:

1. Open a command prompt.
2. Go to the CPinfo tool path location: cd \path\
3. Run CPinfo with output filename and folder:

   ```
   C:\path\>CPinfo.exe <output cab filename> <output folder name>
   ```

   For example: `C:\path\>CPinfo.exe SR1234 temp.`

   The CPinfo application stores the output to the designated folder.

   - If no output name is specified, the output file has the same name as the output folder.
   - If no output folder is specified, `CPinfoPreboot` saves the output file to the directory where the CPinfo tool is located.

Using CPinfoPreboot

Note - CPinfoPreboot does not collect logs from BitLocker-encrypted computers.

Run CPinfoPreboot if you cannot:

- Access the **Pre-boot Logon** window.
- Log in to the **Pre-boot Logon** window.
- Start encryption or decryption.
- You have had a system crash- this includes a Windows or Full Disk Encryption crash.
  - A Windows crash gives you a blue or black screen.
  - A Full Disk Encryption crash gives you a green or red screen.

CPinfoPreboot collects the:

- Readable log of all disks and volumes (`scan.log`).
- Master Boot Record for each disk.
- Partition Boot Record for each volume.
- The first 100 sectors from each physical disk.
- First 100 sectors from each volume.
- System area data.

Use an external USB device to collect the Pre-boot data. The device must have at least 128 MB of free space, and sufficient storage for the output cab file. `CPinfoPreboot` cannot run on boot media prepared with the Full Disk Encryption filter driver

To collect Pre-boot data:

1. Copy `CPinfoPreboot.exe` to an external USB device.
2. Boot the client from the USB device.

   Note - Microsoft Windows does not automatically detect USB devices after boot up. The USB device must be connected while booting the computer.
3. Open the command prompt and type: `<path to CPinfoPreboot> <CPinfoPreboot.exe <output cap filename> <output folder name>.`

   For example: `C:\path\>CPinfoPreboot.exe SR1234 temp.`
4. CPinfoPreboot stores the output file to the designated folder.
   - If no output name is specified, the output file has the same name as the output folder.
   - If no output folder is specified, `CPinfoPreboot` saves the output file to the working directory on the external media. An output folder is required if the working directory is on read-only media.

Debug Logs Collected by CPinfo and CPinfoPreboot

You can use the debug logs to examine the deployment phase or problems that occur. The information there is included in `CPinfopreboot`. Send the full results of `CPinfopreboot` to Check Point Technical Support for analysis.

The client debug log file is on the user's Endpoint Security client computer (for Windows 7 and higher) at:

`C:\ProgramData\CheckPoint\Endpoint Security\Full Disk Encryption`

The log file name is `dlog1.txt`. For BitLocker it is called `Win_Nem.log`. For an explanation of the error messages that can show in Win_Nem.log, see sk157995.

Pre-boot Issues

Note - Pre-boot issues are not relevant for BitLocker-encrypted computers

Mouse or Keyboard Trouble

If users have trouble with their mice or keyboards during Pre-boot, you might need to change the setting of **Enable USB device in Pre-boot environment**. This setting is in the **Full Disk Encryption Policy** > **Pre-boot Settings**. You can also change this setting from the Pre-boot Customization Menu by pressing both shift keys while Full Disk Encryption is loading when the computer starts up.

Trouble with Password on First Pre-boot

When the Pre-boot window opens for the first time on a computer, users get a message to log in with their Windows password. If the Windows password does not meet the requirements configured for the Pre-boot, the authentication does not work.

To resolve this, change the password requirements in the OneCheck User Settings to match the Windows requirements. Then install the new OneCheck User Settings policy on the client.

Trouble with Smart Cards

If there are Smart Card compatibility issues, change the **Legacy USB Support** setting in the BIOS. If it is enabled, change it to disabled, and if disabled, enable it.

If clients have UEFI, see the UEFI Requirements in the *Release Notes for your Endpoint Security client version*.

Full Disk Encryption Logs

Full Disk Encryption utilizes the client logger module for audit logging. Logs are created in the Pre-boot and Windows environments. Logs created in Pre-boot are cached in the Full Disk Encryption system area before they are transferred to the client logger module. Full Disk Encryption logs these operations:

- User acquisition
- Installation and upgrade
- Policy changes
- Dynamic encryption
- User authentication/user locked events

Upgrade Issues

- The `FDEInstallDLL.dll` file creates the upgrade log: `%ALLUSERSPROFILE%\Application Data\Check Point\Full Disk Encryption\FDE_dlog.txt`. Always examine the log file for possible installation errors.
- The log file sometimes contains Win32 error codes with suggested solutions. To show the Win32 error code text, run the `HELPMSG` command: `C:\>net helpmsg <errorcode>`

Full Disk Encryption Deployment Phase Issues

Here are some issues that can occur in the Deployment Phase and possible causes and solutions.

Problem: The deployment is stuck at the user acquisition stage

Causes and Solutions:

1. The User Acquisition policy might say that multiple users must log on to a computer. You can:
   - Change the User Acquisition policy.
   - Instruct users to log on to the computer so Full Disk Encryption can acquire them.
   - Make sure that a user logs on with an account that has a password. User accounts without passwords cannot be acquired.

   If User Acquisition is not enabled, at least one user with a password must be assigned to the device.
2. The Pre-boot password requirements must not be stricter than the Windows logon password requirements. If the password requirements of Windows and the Pre-boot do not match, change the password settings for the Pre-boot password.
3. Make sure that the necessary connections work and that all processes are running. Make sure that:
   - The network connection is stable.
   - Driver Agent is running and has a connection to the server.
   - The Device Auxiliary Framework is running.

Problem: The deployment is stuck at the encryption stage

Causes and Solutions:

If encryption stopped at 50%, make sure that system services are running. Make sure that the `fde_srv.exe` service is running. If it is not running, start it manually (right-click the service and select start in Windows Task Manager).

Problem: The deployment is slow or hanging

Causes and Solutions:

- Make sure that the computer has all client requirements.
- Disk fragmentation or a damaged hard drive can cause problems with Full Disk Encryption. Run disk defragmentation software on the volume to repair fragmentation and damaged sectors.
- Make sure that the network connection is stable.

User Authentication to Endpoint Security Clients (OneCheck)

OneCheck User Settings define how users authenticate to Endpoint Security client computers.

OneCheck User Settings include:

- How users authenticate to Endpoint Security.
- If users can access Windows after they are authenticated to Endpoint Security or if they must also log on to Windows.
- What happens when a user enters invalid authentication details.
- A limit for how many times a user can access a computer.
- If Remote Help is permitted. This lets users get help from an administrator, for example if their computers become locked after too many failed authentication attempts.

Configure the OneCheck User Settings setting in the **Policy** tab > **OneCheck User Settings** Rules.

Many of these settings relate to the Pre-boot authentication, which is part of Full Disk Encryption. Make sure to configure the settings for the Full Disk Encryption Policy also in **Policy** tab > **Full Disk Encryption** Rules.

Configuring OneCheck User Settings Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

Pre-boot Authentication Methods

If the Pre-boot is required on a computer as part of Full Disk Encryption, users must authenticate to their computers in the Pre-boot, before the computer boots. Users can authenticate to the Pre-boot with these methods:

- **Password** - Username and password. This is the default method.

  The password can be the same as the Windows password or created by the user or administrator.

- **Smart Card** - A physical card that you associate with a certificate. This is supported in E80.30 clients and higher.

  Users must have a physical card, an associated certificate, and Smart Card drivers installed.

- **Dynamic Token** - A physical device that generates a new password each time users start their computers. This can be configured for specified users and not as the global Pre-boot authentication method.

Configure the global settings for the Pre-boot authentication method from the **OneCheck User Settings Actions**.

Global Pre-boot Authentication Settings

Configure the global settings for the Pre-boot authentication method from the **OneCheck User Settings** policy rule. The settings configured here apply to all users. You can override the global settings for specified users.

Select an Action to define the default Pre-boot authentication method:

Action	Description
Authenticate users with Password	Users can only authenticate with a username and password.
Authenticate users using Smart Card or Password	Users can authenticate with either username and password or Smart Card.

The password settings are taken from the OneCheck User Settings rules that are assigned to the user.

Right-click an Action and select **Edit** to configure more settings if you select to use Smart Card authentication.

Important - Before you configure Smart Card authentication only as the default, make sure that you understand the requirements. See *"Before You Configure Smart Card Authentication" on page 273*. All requirements must be set up correctly for users to successfully authenticate with Smart Cards.

To configure Smart Card only or for Smart Card or Password as the default:

1. Select one of the Smart Card options as the **Default Pre-boot authentication method**.
2. If you select **Smart Card**, we recommend that you select **Change authentication method only after user successfully authenticates with a Smart Card**

   This lets users authenticate with a password until all of the requirements for Smart Card authentication are set up correctly. After users successfully authenticate one time with a Smart Card, they must use their Smart Card to authenticate. If you configure a user for Smart Card only and do not select this, that user is not able to authenticate to Full Disk Encryption with a password.

   Select one or more Smart Card drivers.
3. In the **Smart Card driver** area, select the Smart Card protocol that your organization uses:
   - **Not Common Access Card (CAC)** - all other formats
   - **Common Access Card (CAC)** - the CAC format
4. In the **Select Smart Card driver to be deployed** area, select the drivers for your Smart Card and Reader. All selected drivers will be installed on endpoint computers when they receive policy updates.

   If you do not see a driver required for your Smart Card, you can:
   - Enter a text string in the **Search** field.
   - Click **Import** to import a driver from your computer. If necessary, you can download drivers to import from the Check Point Support Center.
5. In the Directory Scanner area, select **Scan user certificates from Active Directory** if you want the Directory Scanner to scan user certificates.
6. If you selected to scan user certificates, select which certificates the Directory Scanner will scan:

- **Scan all user certificates**
- **Scan only user certificates containing the Smart Card Logon OID** - The OIDs are: 1.3.6.1.4.1.311.20.2.2.

7. Click **OK**.

If necessary, use the Pre-boot Reporting reports to troubleshoot issues with drivers or user certificates.

Changing the User Pre-boot Authentication Settings

By default, users get the Pre-boot authentication method from the global Pre-boot Authentication Settings. You can assign custom authentication settings to users on the **User Details** page. You can also assign a user password and manually add user certificates on this page.

You can assign **Dynamic Token** as a user's authentication method.

To change a user Pre-boot authentication method:

1. Double-click a user in the tree.
2. In the **User Details** window, select **OneCheck User Settings**.
3. Click **Pre-boot Authentication Method**.
4. Click **Use specific Pre-boot Authentication Method for this user**.
5. Select an authentication method:
   - **Password** - This user can only authenticate with a username and password.
   - **Smart Card** - This user can only authenticate with a Smart Card.
   - **Either Smart Card or Password** -This user can authenticate with user name and password or a Smart Card.
   - **Dynamic Token** - This user can only authenticate with the password from a dynamic token.
6. If you select **Smart Card**, we recommend that you select **Change authentication method only after user successfully authenticates with a Smart Card**

   This lets users authenticate with a password until all of the requirements for Smart Card authentication are set up correctly. After users successfully authenticate one time with a Smart Card, they must use their Smart Card to authenticate. If you configure a user for Smart Card only and do not select this, that user is not able to authenticate to Full Disk Encryption with a password.

   Select one or more Smart Card drivers.

7. If you select Dynamic Token, click **Select token**. The user can only authenticate with the selected token. See *"Managing Dynamic Tokens" on page 277*.
   - Select a token from the list or click **Add** or **Import** to add a new token.
   - Click **OK**.
8. Click **OK**.
9. On the **OneCheck User Settings** page:
   - For **Password** authentication - You can enter a **User Password** or **Change Password**.
   - For **Smart Card** authentication - In the **User Certificates** area, make sure the user has a valid certificate to use with the Smart Card. If a certificate is not shown, you can click **Add** to import a certificate.

Password Complexity and Security

Policy view > **OneCheck**

These Actions define the requirements for user passwords for OneCheck User Settings:

Action	Description
Use Windows password complexity	The standard Windows password requirements are enforced: The password must: ■ Have at least six characters ■ Have characters from at least 3 of these categories: uppercase, lowercase, numeric characters, symbols.
Use custom password complexity	If you select this, select the requirements for which type of characters the password must contain or not contain.

Double-click an action to edit the properties:

Option	Description
Use custom requirements	If you select this, select the requirements for which type of characters the password must contain or not contain: ■ Consecutive identical characters, for example, aa or 33 ■ Require special characters. These can be: `~ = + - _ ( ) ' $ @ , .` ■ Require digits, for example 8 or 4. ■ Require lower case characters, for example g or t. ■ Require upper case characters, for example F or G. ■ Password must not contain user name or full name.
Minimum length of password	Enter the minimum number of characters for a valid password.
Password can be changed only after	Enter the minimum number of days that a password must be valid before the user can change it.
Password expires after	Enter the maximum number of days that a password can be valid before the user must change it.
Number of passwords	Enter the minimum number of password changes needed before a previously used password can be used again.

Password Synchronization

Pre-boot is a program that prevents the operating system from booting until the user authenticates. You can synchronize the Pre-boot and operating system passwords.

Notes and Recommendations:

- Password Synchronization only works if Pre-boot authentication is enabled.
- If you plan to use OneCheck Logon, we recommend that you keep the OS and Pre-boot passwords synchronized. This makes sure that both passwords are the same, and users can use each one, if necessary.
- If you use password synchronization, we recommend that users' Windows password and Pre-boot password have the same requirements. This prevents problems with the first Pre-boot logon, OneCheck Logon, and Single Sign-On.
- If the OneCheck User Settings policy is set to synchronize Pre-boot and Windows passwords, and a user changes his or her password, the change is automatically sent to all computers the user is authorized to access in Pre-boot.

  The password change is communicated to relevant clients as part of the regular heartbeat and sync messages between clients and servers. If a computer is not connected to an Endpoint Security Server when the password is changed, the change is sent to the computer after it connects to an Endpoint Security Server.

  In this situation, users might have to log in to Pre-boot one time with their old passwords before the client can connect to the server and get the updated credentials.

Select an Action to define if and how the passwords are synchronized:

Action	Description
Update Pre-boot password Upon Windows Password Change	When the OS password on a computer changes, the Pre-boot password is automatically changed.
Update Windows Password Upon Pre-boot Password Change	When the Pre-boot password on a computer changes, the OS password is automatically changed.
Bi-directional Update for Pre-boot and Windows Password Upon Change	If the Pre-boot or OS password on a computer changes, the password is automatically changed.
Do Not Synchronize Pre-boot and Windows passwords	The Pre-boot and OS passwords on a computer are not synchronized by Endpoint Security.

Account Lock

You can configure Full Disk Encryption to lock user accounts after a specified number of unsuccessful Pre-boot login attempts:

- **Temporarily** - If an account is locked temporarily, users can try to log on again after a specified time.
- **Permanently** - If the account is locked permanently, it stays locked until an administrator unlocks it.

Select one of these Actions to define if and when user accounts are locked:

Action	Description
Do not lock out users upon failed authentication.	Users are not locked out of their accounts if they try to log on unsuccessfully. This setting is not recommended.
Temporarily lock user account upon failed authentication attempts	After a configured amount of failed log on attempts (the default is 5), the user's account is temporarily locked.
Permanently lock user account upon failed authentication attempts	After a configured amount of failed log on attempts (the default is 10), the user's account is permanently locked.

Right-click an Action to edit the properties. You can also create custom Account Lock actions.

To configure an Account Lock Action:

1. Right-click the existing Action and select **Edit Properties** or select **Create Custom** to define a new Action.
2. Configure the settings as necessary:

Option	Description
Number of failed logons before the account is locked	Maximum number of failed logon attempts allowed before an account is permanently locked. The account is locked until an administrator unlocks it.
Number of failed attempts before a temporary lockout	Maximum number of failed logon attempts before an account is temporarily locked out.

Option	Description
Duration of a temporary lockout	Duration of a temporary lockout period, in minutes.
Maximum number of successful logons allowed before the account is locked	Maximum number of successful logins before an account is permanently locked. You can use this option to let a temporary user log in for a specified number of logins. To unlock an account, you must increase the value or clear this option. Remote Help is not available for this type of account lockout.

Logon Settings

OneCheck User Settings **Logon Settings** define additional settings for how users can access computers. Expand the **Advanced section** in the OneCheck User Settings rule to configure this.

Option	Description
Allow logon to system hibernated by another user	Lets a different user than the logged on user authenticate in Pre-boot to a system in hibernate mode.
Allow use of recovery media	Let user authenticate to use recovery media to recover and decrypt data from an encrypted system. **Note:** In E80.20 and higher, if this is not selected, users can still access recovery media that is created with a temporary user and password.
Allow user to change his credentials from the endpoint client	Let users change the password on an endpoint client during the Pre-boot.
Allow Single Sign-On use	Let users use Single Sign On to log on to Pre-boot and Windows when OneCheck Logon is disabled. Single Sign on applies only to Pre-boot and Windows and not to different components, such as VPN or Media Encryption. Users are always allowed to use Single Sign On when OneCheck Logon is running.

Remote Help Permissions

Remote Help lets users access to their Full Disk Encryption protected computers if they are locked out. The user calls the designated Endpoint Security administrator and does the Remote Help procedure. Expand the **Advanced section** in the OneCheck User Settings rule to configure this.

There are two types of Full Disk Encryption Remote Help:

- **One Time Login** - One Time Login allows access as an assumed identity for one session, without resetting the password.

  If users lose their Smart Cards, they must use this option.

- **Remote password change** - This option is for users who use fixed passwords and have forgotten them.

For devices protected by Media Encryption & Port Protection policies, only remote password change is available.

To let users work with Remote Help:

1. Make sure **Allow remote help** is selected in **OneCheck User Settings** rule> **Advanced** > **Allow remote help**.
2. Optional: Edit the properties to allow only one type of Remote Help.

Option	Description
Allow account to receive remote password change help	Let users get help from an administrator to reset the account password (for example, if the user forgets the password).
Allow account to receive One-Time Logon help	Let the user get help from an administrator to log on, one time. One-time logon is for users who have lost their dynamic tokens, USB tokens, or Check Point Smart Card. It is also useful if the user made too many failed attempts but does not want to change the password.

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 1000, a message shows that only the first 1000 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 1000. 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 1000 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 **OneCheck User Settings**.

- 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.

Creating Pre-boot Users

Pre-boot users can be within a node or not assigned to a node.

To create new online Pre-boot user:

1. in the **Users and Computers** tab, right-click on an OU under **Directories** or **Other Users/Computers**.
2. Select **User Authentication (OneCheck) > Authorize Pre-boot Users**.
3. Click **New**.

   The **Add new Pre-boot user** window opens.
4. Enter a **Logon Name**
5. In the **Authentication credentials** area, select **Password** or **Dynamic Token**.
   - A password must contain at least five characters
   - If you select an token as the authentication method, make sure you select an existing token
6. 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.
7. 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 unlink a Windows user from the logged on Pre-boot account:

1. From an Endpoint Security client, open the client **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.

AD Groups for Pre-boot Authentication

You can add Active Directory users and groups to devices, OUs, or groups for Pre-boot authentication. In SmartEndpoint, groups have an 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 1000.

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 **OneCheck User Settings** > **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**.
5. If a user does not have configured credentials, a **User Logon Pre-boot Settings** window opens. Configure credentials in the window. 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 1000, the operation is blocked.

Before You Configure Smart Card Authentication

Make sure the environment is set up correctly to use Smart Card authentication before you configure it.

To use Smart Card authentication, you must have these components and requirements:

- Smart Card authentication is only supported on Endpoint Security clients of version E80.30 or higher. Make sure all users have a supported version.

  You can see which versions users have in the **Endpoint Security Management Console** > **Monitoring** tab > **Versions in Use**.

- Users must have the physical Smart Card in their possession.
- Users' computers must have a Smart Card reader driver and token driver installed for their specific Smart Card. Install these drivers as part of the global **Pre-boot Authentication Settings**.
- Each user must have a certificate that is active for the Smart Card.
  - The Directory Scanner can scan user certificates from the Active Directory. Configure this in the global **Pre-boot Authentication Settings**.
  - You can manually import a certificate for a user in **User Details** > **Security Blades** > **OneCheck User Settings**.
- In a Full Disk Encryption Policy rule, open the **Authenticate user before OS loads** action. Click on **Advanced Pre-boot Settings** and make sure that **Enable USB devices in pre-boot** environment is selected.

Smart Card Scenarios

Below are scenarios of how to implement Smart Card authentication in organizations with different needs.

Scenario 1: Moving from Password to Smart Card

Scenario

Your organization uses Check Point Endpoint Security with username and password authentication for Full Disk Encryption Pre-boot. You want to move all users to Smart Card authentication for even greater security. Your organization uses Active Directory.

What to do:

1. Plan your Smart Card environment:
   - Give all users a Smart Card.
   - Get a Smart Card certificate for each user and put them in Active Directory.
   - Learn which Smart Card driver and Reader driver is necessary for your Smart Card.
2. Upgrade all endpoints to this version. Use **Reporting** reports to make sure all users are successfully upgraded.
3. Open the **Policy** tab.
4. In a **OneCheck User Settings** rule, right-click the **Authenticate users** action and select **Edit**:
   - Select **Smart Card (requires certificates)**.
   - Select **Change authentication method only after user successfully authenticates with a Smart Card**.
   - Select the drivers required for your Smart Card.
5. In the **Directory Scanner** area, click **Configure**.

   The **Certificate Scanning Configuration** window opens.
6. Select **Scan user certificates from Active Directory**.
7. Monitor the Smart Card deployment in the Pre-boot Reporting reports.
8. If you choose, you can clear the **Change authentication method only after user successfully authenticates with a Smart Card** option after all users have logged on with their Smart Card. If a specified user must use password authentication temporarily, you can change the Pre-boot Authentication Settings for the user to **Password**.

Scenario 2: Mix of Password and Smart Card Authentication

Scenario

Your organization is preparing to install Check Point Endpoint Security for the first time. Most users will use username and password Pre-boot authentication. Administrators with high administrative privileges will use Smart Card authentication. Your organization does not use Active Directory.

What to do:

1. Plan your Smart Card environment.
   - Give a physical Smart Card to all users who will use a Smart Card.
   - Get a Smart Card certificate for each user who will use a Smart Card.
   - Learn which Smart Card driver and Reader driver is necessary for your Smart Card.
2. Deploy the Endpoint Security client, including Full Disk Encryption on all endpoints. See *"Deploying Endpoint Security Clients" on page 133*. Use Reporting reports to make sure that Full Disk Encryption completes the deployment phase and the **Full Disk Encryption Status** of each computer is **Encrypted**.
3. Open the **Policy** tab.
4. In a **OneCheck User Settings** rule, select one of the **Authenticate users** actions:
   a. Select **Authenticate users with Password** and manually configure the Smart Card users to use Smart Card authentication.
   b. Select **Authenticate users using Smart Card or Password**. For added security, you can manually configure each Smart Card user to use Smart Card authentication only.
5. Right-click the **Authenticate users** action and select **Edit**.
6. Select the drivers required for your Smart Card and the Smart Card protocol. All users will receive these settings, including those who are configured to use Password authentication.
7. In the OneCheck User Settings page for each Smart Card user, in the **User Certificates** area, click **Add** to import a certificate.
8. Monitor the Smart Card deployment in the Pre-boot Reporting reports.

Note - You can put all Smart Card users in a virtual group so that it is easy to monitor them and change their policies, if necessary.

Notes on Using Smart Cards

- Check Point does not supply Smart Card features to use with Windows. You can use third-party software, supplied by Windows or the Smart Card vendor.
- To use recovery media with a Smart Card-only user, when you create the recovery media, create a temporary user who can authenticate to it.

Changing a User's Password

Users can change their own passwords from the Pre-boot. You can manage user Pre-boot passwords from the **User Details** window.

To change a user's Pre-boot password from SmartEndpoint:

1. In the **User Details** > **Security Blades** > **OneCheck User Settings** in the Pre-boot authentication method area, click **Change Password**.
2. In the **Change User Password** window, enter the new password and re-enter it.
3. Click **OK**.
4. Click **OK**.
5. Select **File** > **Save**.

Managing Dynamic Tokens

Manage the tokens that users can use in SmartEndpoint.

Adding a Token

To add a dynamic token:

1. In SmartEndpoint, go to **Manage > Dynamic Token Management**.
2. Click **Add**.

   The **Add Token** window opens.
3. Enter relevant values:

Field	Description	Valid parameters
Dynamic Token Serial Number	Unique serial number identifying this token.	
Algorithm	Cryptography algorithm that this token implements.	DES 3DES
Dynamic Token Key	Token key used for this account.	DES: 14 characters long 3DES: 42 characters long Contains digits 0-9 and letters A-F
Response Length	Number of characters in the ASCII response string.	8 16
Challenge Format	Format of ASCII challenge string.	Hexadecimal Decimal
Challenge Length	Number of characters in the ASCII challenge string.	8 16
Response Format	Format of ASCII response string.	Friendly Decimal
Comment	Optional text.	ASCII text

4. Click **OK**.

Removing a Token.

To remove a dynamic token:

1. In SmartEndpoint, go to **Manage > Dynamic Token Management**.
2. Select a token you want to remove.
3. Click **Remove**.

   The token is removed immediately.

   Important - After a token is removed, it cannot be restored.

Importing Tokens

To import tokens:

1. In SmartEndpoint, go to **Manage > Dynamic Token Management**.
2. Click **Import**.

   The **Token Import Wizard** window opens.
3. Select an `.imp` file.

   You can navigate to the location of the file through a windows explorer, by typing in a full path name, or drag and drop the file into the field in the wizard.
4. Click **Next**.

   Tokens in the selected file show on the list.
5. Select tokens to import.
6. Enter the password for the `.imp` file.
7. Click **Next**.

   Decrypted tokens show on the list.
8. Select decrypted tokens.
9. Click **Finish**.

Upgrading Legacy Token Users

This upgrade helps resolve issues with users and systems in unmanaged legacy (pre-E80) token deployment environments.

To upgrade legacy token users:

Set the value of `AllowTokenUpgrade` in the Full Disk Encryption registry key. Refer to sk95466.

Media Encryption & Port Protection

The Media Encryption & Port Protection component protects sensitive information by encrypting data and requiring authorization for access to storage devices, removable media and other input/output devices. Administrators use the SmartEndpoint to create rules for data encryption, authorization and access to devices. These rules are part of the Endpoint Security policy installed on endpoint computers.

Media Encryption & Port Protection rules include these settings:

- Default actions for reading and writing to different types of devices.
- Read and write access permissions to storage devices.
- Ability to access devices from endpoint computers.
- Types of files that must be encrypted (Business Related Data) on storage devices.
- Offline Access to encrypted devices on computers that are not connected to an Endpoint Security Management Server or on non-protected computers.
- Ability of users to temporarily override rules using UserCheck.

To learn more about how users interact with Media Encryption & Port Protection, see the *Client User Guide for your client release*.

Media Encryption & Port Protection Terminology

Storage Device -Removable media device on which users can save data files. Examples include: USB storage devices, SD cards, CD/DVD media and external disk drives.

Peripheral Device - Devices on which users cannot save data and that cannot be encrypted.

Device Category - Also called Device Class, an Industry standard device type that identifies the base functionality of a storage or peripheral device.

Media Owner - By default, this is the user who encrypts the device. If allowed by the policy, a different user can be assigned to be the media owner. This term applies only to users in Active Directory environments.

Business-Related Data - Confidential data file types that are usually encrypted in the business-related drive section of storage devices in Media Encryption & Port Protection.

UserCheck - Gives users a warning when there is a potential risk of data loss or security violation. This helps users to prevent security incidents and to learn about the organizational security policy.

Explorer Utility - Software that lets users read encrypted data on Endpoint Security-protected computers on which the Media Encryption component is not active or not connected to an Endpoint Security Management Server.

Working with Actions in a Media Encryption & Port Protection Rule

Each Media Encryption & Port Protection rule includes these main action types:

- *"Configuring the Read Action" on page 283* - Controls how users can read devices that are protected by the policy
- *"Configuring a Write Action" on page 284* - Controls how and when users can write to devices that are protected by the policy
- *"Configuring Peripheral Device Access" on page 288* - Controls access to different types of peripheral devices

Media Encryption & Port Protection rules also contain these **Advanced** action types:

- *"Offline Access Actions" on page 295* - Controls access to devices that are connected a non-protected computer
- *"Device Scanning and Authorization Actions" on page 300* - Configures scanning of storage devices for malware and unauthorized file types.
- *"Log Actions" on page 303* - Controls when Media Encryption & Port Protection creates log entries when a storage device is attached to an endpoint computer
- *"UserCheck Actions" on page 305* - Controls when and how to tell users about policy violations and optionally lets them override a policy.
- *"Media Encryption Site Actions" on page 306* - Controls when to allow or prevent access to drives encrypted by different Endpoint Security Management Servers
- *"Global Automatic Access Action" on page 309* - Defines the default automatic action that applies to all rules, unless overridden by a different rule or action.

Configuring the Read Action

The Read Action defines the default settings for read access to files on storage devices. For each action, you can define different settings for specified device types.

The default predefined actions are:

Action	Description
Allow reading any data from storage devices	Allow users to read encrypted and non-encrypted data from storage devices.
Allow reading only encrypted data from devices	Allow users to read only encrypted data from storage devices. Users cannot read unencrypted (Non-Business related) data.
Do not allow reading from any storage device	Block reading from all storage devices.

You can also create your own custom actions. Your new custom actions are always available in addition to the default actions.

To configure a Read Action:

1. Right-click **a Read Access** action in a rule and select **Edit Properties**.
2. **Optional**: In the **Removable Media Read Access** window, select a different action or click **New**.

   If you click **New**, enter a name and description for the new action.
3. Enable these options as necessary:
   - **Allow reading unencrypted data from storage devices** - Users can read unencrypted (typically Non-Business Related) data.
   - **Allow reading encrypted data from storage devices** - Users can read encrypted (typically, but not always, Business Related data).
4. Add or change *"Defining Exceptions for Devices " on page 290*.

Configuring a Write Action

You define the default settings for write access to storage devices in the **Removable Media Write Access** window.

This action can let users:

- Create new files
- Copy or move files to devices
- Delete files from devices
- Change file contents on devices
- Change file names on devices

The default predefined write actions are:

Action	Description
Allow writing any data to storage devices	Users can write all file types to storage devices.
Encrypt business related data written to storage devices	All Files that are defined as Business related data must be written to the encrypted storage. Non-business related data can be saved to the device without encryption. See *"Configuring Business Related File Types" on page 286*.
Encrypt all data written to storage devices	All files written to a storage device must be encrypted. This includes both Business and Non-Business Related data.
Do not allow writing any data to storage devices	Users cannot write any file types to storage devices.
Do not allow writing any data to storage devices, allow user override	By default, users cannot write any file types to storage devices. But, UserCheck lets users override the policy and write to a storage device, after entering justification for the action.

You can define custom write actions as necessary. Your new custom actions are always available in addition to the default actions.

To configure a storage device Write Action:

1. Right-click a **Write Access** action and select **Edit Properties**.

   The **Removable Media Access** window opens.

2. **Optional**: Select a different action from the list.

   Click **New** to create a custom action.

3. Select one of these **Storage device write access** options:

   - **Allow any data** - Users can write all data types to storage devices.
   - **Encrypt business related data** - Users can write all data types to the storage devices. Only Business Related data must be encrypted.
   - **Encrypt all data** - Users can write all data types to storage devices. All data must be encrypted, including Non-Business Related data.
   - **Block any data** - Users cannot write to the storage devices.

4. Select one or more of these options:

   - **Log device events** - Select this option to create a log entry when a storage device is attached (Event IDs 11 and 20 only).

     Note: If you do not select the **Log device events** option in the Media Encryption & Port Protection rule, log entries are not created even if the **Audit device events** option is selected in this window.

   - **Allow encryption** - Select this option to let users encrypt storage devices. If this option is cleared, no storage devices can be encrypted.

     Click **Additional Encryption Options** to configure additional encryption settings as necessary (see *"Offline Access Actions" on page 295*).

   - **Enable deletion** - Select this option to let users delete files on devices with read only permissions.

5. Configure these settings for **User Overrides (UserCheck)**

   - **Allow user to override company policy** - Lets users override the assigned policy by sending written justification to an administrator.

     Click **Configure Message** to create your own user message (see *"Creating a Custom User Message" on page 287*).

     Note - The **Allow user to override company policy** option is not supported for CD/DVD ROM devices.

6. If necessary, click **Configure file types** to define custom business related file types (see *"Configuring Business Related File Types" on the next page*).

Configuring Business Related File Types

If you enable the **Encrypt business-related data written to storage devices** option, users must encrypt all file types that are defined as business-related. Users can save non business-related file types without encryption.

If you enable the **Force encryption of all outgoing data** option, all data, including Non-Business related data, must be encrypted.

- **Business Related data** - Confidential data file types that must be encrypted on removable media. Examples include: word processor files, spreadsheet files, presentations and drawings.
- **Business Related drive** - The encrypted portion of a drive (up to 100% of the device). All data that is stored on the Business Related portion is encrypted.
- **Non-Business Related data** or **Plain** - File types that are not confidential and do not require encryption on storage devices.
- **Non-Business Related drive** - The unencrypted portion of a drive (if less than 100% is encrypted). Data stored on the Non-Business Related portion is not encrypted.

There are predefined categories of similar file types. You cannot change the file types included in these groups, but you can create your own custom groups. This list includes some of the predefined file type groups:

These groups are defined as Business Related by default:

- **Word** - Word processor files, such as Microsoft Word.
- **Spreadsheet** - Spreadsheet files, such as Microsoft Excel.
- **Presentation** - Presentation files, such as Microsoft Power Point.
- **Database** - Database files, such as Microsoft Access or SQL files.
- **Drawing** - Drawing or illustration software files, such as AutoCAD or Visio.
- **Graphic** - Graphic software files such as Photoshop or Adobe Illustrator.
- **Viewer** - Platform independent readable files, such as PDF or Postscript.
- **Archive** - Compressed archive files, such as ZIP or SIT.
- **Markup** - Markup language source files, such as HTML or XML.
- **Email** - Email files and databases, such as Microsoft Outlook and MSG files.
- **Text** - Plain text files.

Groups defined as Non-Business Related by default

- **Multimedia** - Music and video files, such as MP3 or MOV.
- **Image** - Vector image files such as JPG or PNG.
- **Executable** - Executable program files, such as EXE or COM.

To classify groups as Business or Non-Business Related:

1. Click a write action and select **Edit Properties**.
2. In the **Removable Media Write Access** window, select **Encrypt business related data written to storage devices**.
3. Click the **Configure Business Related file types** link.
4. On the **Business Related File Types** page, select **Business-related** or **Non business-related**.
5. Click **Add** to add a group to the list.
6. Click **Remove** to remove a group from the list.

Creating a Custom User Message

You can customize the text that shows in all sections of the user message window, including the banner and the option buttons. You cannot change the Check Point logos. . This feature is useful for translating user messages into different languages.

To create a custom user message:

1. In the **Select User Message** list, select **New**.
2. Enter a name and description in the applicable fields in the **Policy Action Single Page Form** window.
3. Optional: Select a language from the **Language** list.

   You can click **Add** to add another language to the list.
4. Select one or more text elements and enter your custom text.
5. Click **Preview** to see how the custom message shows on the screen.

Configuring Peripheral Device Access

Peripheral devices cannot be encrypted and do not contain storage. These predefined actions define which peripheral devices can be used with an endpoint computer.

Action	Description
Allow connecting essential devices (keyboard, mouse, and network adapters)	Access to necessary peripheral devices for basic computer functionality is allowed. Other peripheral devices are blocked.
Block all transmitting devices (Modem, Bluetooth, IrDA, Wi-Fi)	Access to transmitting peripheral devices is blocked. Other peripheral devices are allowed.
Allow connecting all peripheral devices	Access to all devices that cannot be encrypted or do not contain storage is allowed.

You can also create and change your own custom actions.

Creating a Custom Action

To create a new custom action:

1. In the Media Encryption & Port Protection rule, right-click the Peripheral Device action and select **Create Custom**.
2. In the **Peripheral Device Access** window, enter a unique action name and, optionally, textual comments.
3. For each device in the list, change the **Access Type** as necessary (**Allow** or **Block**).
4. For each device in the list, change the **Log** settings as necessary:
   - **Log** - Create log entries when a peripheral device is connected to an endpoint computer (Action IDs 11 and 20)
   - **None** - Do not create log entries
5. **Optional**: Add new devices as necessary.

Changing an Existing Action

To change an existing action definition:

1. In the Media Encryption & Port Protection rule, right-click an action and select **Edit Properties**.

2. In the **Peripheral Device Access** window, click **Edit Name & Description** and change settings as necessary.
3. For each device in the list, change the **Access Type** as necessary (**Allow** or **Block**).
4. For each device in the list, change the **Log** settings as necessary:
   - **Log** - Create log entries when a peripheral device is connected to an endpoint computer (Action IDs 11 and 20)
   - **None** - Do not create log entries
5. **Optional**: Add new devices as necessary.

Defining Exceptions for Devices

You can configure custom settings for specified devices or device types. These device settings are typically used as **exceptions** to settings defined in Media Encryption & Port Protection rules.

You can define device-specific exceptions for:

- One device, which is based on its serial number.
  You must enter the device serial number.
- A device model, which is based on the device ID.
  You must enter the device ID.
- A device type, such as Windows Portable Devices or Imaging Devices.
- A user defined device group (storage devices only).

Editing Device Details

These properties are configured for each device that is connected to a client with Media Encryption & Port Protection:

- **Device Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Device Connection** - Select the connection type **Internal**, **External** or **Unknown** (required).
- **Device Category** - Select a device category from the list.
- **Device Serial Number** - Enter the device serial number. You can use wild card characters in the serial number to apply this device definition to more than one physical device. See *"Using Wild Card Characters" on page 293*
- **Extra Information** - Configure whether the device shows as fixed disk device (**Hard Drive with Master Boot Record)**, a removable device (**Media without Master Boot Record**) or **None**.
- **Icon** - Select an icon to show in the GUI.
- **Device ID Filter** - Enter a filter string that identifies the device category (class). Devices are included in the category when the first characters in a **Device ID** match the filter string. For example, if the filter string is `My_USB_Stick`, the following devices are members of the device category:

  ```
  My_USB_Stick_40GB
  ```

  ```
  My_USB_Stick_80GB
  ```

- **Allow encryption** - Select this option if the device can be encrypted (storage devices only).
- **Can generate device arrival audit event** - Select this option to create a log entry when this device connects to an endpoint computer (Event ID 11 or 20 only).

Creating a Device with Automatic Device Discovery

You can use the **Device Discovering Wizard** to create new devices that have been connected to endpoint computers.

To create a device with the Device Discovering Wizard:

1. Open the **Storage Devices Read Access, Storage Devices Write Action, or Peripheral Devices Access** action.
2. In the **Device Overrides** section of the **Edit Properties** window, click **Add device**.
3. In the **Device Override Settings** window, select **Create a new device**.
4. Click **Next**.
5. Select **Add discovered device from user logs**.
6. Click **Next**.
7. Select a device from the list. If necessary, search or filter to find the device.
8. Click **Next**.
9. **Optional**: Edit the device details. See *"Editing Device Details" on the previous page*.
10. Click **Next**.
11. Optional: Add this device to one or more device groups (storage devices only).
12. Click **Next**.
13. Define the behavior of the device. The options shown are based on which action you are editing:
    - For Storage Devices Write Access see *"Configuring a Write Action" on page 284*.
    - For Storage Device Read Access see *"Configuring the Read Action" on page 283*.
    - For Peripheral device access:
      - **Access type**: Block or Allow
      - **Log type**: Log or None
14. Click **Finish**.

Creating a Device Manually

You can manually define a device that was not inserted into a client computer.

To manually create a new device:

1. Open the **Storage Devices Read Access, Storage Devices Write Action, or Peripheral Devices Access** action.
2. In the lower section of the **Edit Properties** window, click **Add device**.
3. In the **Device Override Settings** window, select **Create a new device**.
4. Click **Next**.
5. Select **Manually configure device**.
6. Click **Next**.
7. Enter the device details. *"Editing Device Details" on page 290*
8. Click **Next**.
9. Optional: Add this device to one or more device groups (storage devices only).
10. Define the behavior of the device. The options shown are based on which action you are editing:
    - For Storage Devices Write Access see *"Configuring a Write Action" on page 284*
    - For Storage Device Read Access see *"Configuring the Read Action" on page 283*.
    - For Peripheral device access:
        - **Access type**: Block or Allow
        - **Log type**: Log or None
11. Click **Finish**.

Editing Device Access Setting

You can change the settings for an individual device or category of devices.

To change the access settings for existing devices from the Policy Rule Base:

1. Open the **Storage Devices Read Access, Storage Devices Write Action, or Peripheral Devices Access** action.
2. In the **Device Overrides** area of the **Edit Properties** window, select a device or group and click **Edit device**.

3. If you selected a group, **Add** or **Remove** objects until the **Selected Objects** list contains all applicable devices.
4. Select or clear these options as applicable. The options that show are based on the action you are working with.
   - For Storage Devices Write Access see *"Configuring a Write Action" on page 284*.
   - For Storage Device Read Access see *"Configuring the Read Action" on page 283*.
   - For Peripheral device access:
     - **Access type**: Block or Allow
     - **Log type**: Log or None
5. Click **OK**.
6. Click **OK**.

To change the access settings for devices from the Reporting tab:

1. In the **Reporting** tab > **Media Encryption & Port Protection**, right-click a device and select **Add device as exception**.

   The **Device Override Settings** open.
2. Edit the device details as necessary. See *"Editing Device Access Setting" on the previous page*

Using Wild Card Characters

You can use wild card characters in the **Device Serial Number** field to apply a definition to more than one physical device. This is possible when the device serial numbers start with the same characters.

For example: If there are three physical devices with the serial numbers 1234ABC, 1234BCD, and 1234EFG, enter 1234* as the serial number. The device definition applies to all three physical devices. If you later attach a new physical device with the serial number 1234XYZ, this device definition automatically applies the new device.

The valid wild card characters are:

The '*****' character represents a string that contains one or more characters.

The '**?**' character represents one character.

Examples:

Serial Number with Wildcard	Matches	Does Not Match
1234*	1234AB, 1234BCD, 12345	1233
1234???	1234ABC, 1234XYZ, 1234567	1234AB, 1234x, 12345678

Because definitions that use wildcard characters apply to more endpoints than those without wildcards, rules are enforced in this order of precedence:

1. Rules with serial numbers containing ***** are enforced first.
2. Rules with serial numbers containing **?** are enforced next.
3. Rules that contain no wildcard characters are enforced last.

For example, rules that contain serial numbers as shown here are enforced in this order:

1. 12345*
2. 123456*
3. 123???
4. 123456?
5. 1234567

Working with Advanced Actions in a Media Encryption & Port Protection Rule

You can configure advanced actions in a Media Encryption & Port Protection policy rule.

Offline Access Actions

You can select one of these predefined actions to define encryption behavior for storage devices:

- **Allow offline access to encrypted media** - Users can enter a password to access storage devices on protected computers not connected to an Endpoint Security Management Server (Offline). Users can also use their password to access storage devices on a non-protected computer.
- **Do not allow offline access to encrypted media** - Users cannot access storage devices on protected computers that are not connected to an Endpoint Security Management Server or on non-protected computers.

You can change the settings of these predefined actions and create new custom **Offline Access to Media** action.

Custom Offline Access Settings

You can define custom offline access actions that include these settings:

Encryption Settings

Setting	Description
Allow user to choose owner during encryption	Lets users manually define the device owner before encryption. This lets users create storage devices for other users. By default, the device owner is the user who is logged into the endpoint computer. The device owner must be an Active Directory user.
Allow user to change size of encrypted media	Lets users change the percentage of a storage device that is encrypted, not to be lower than **Minimum percentage of media capacity used for encrypted storage** or **Default percentage of media capacity used for encrypted storage**. Also see *"Configuring Encryption Container Settings" on page 297*.
Allow users to remove encryption from media	Lets users decrypt storage devices.

Setting	Description
Allow user to upgrade from legacy drives	Lets users upgrade storage devices that were encrypted by File Encryption version R73.
When encrypting, Non-Business Related Data will be:	Select one of these actions for existing data on a storage device upon encryption: ■ **Copied to encrypted section** - Non-Business Related data is encrypted and moved to the Business Related (encrypted) storage device. We recommend that you back up Non-Business Related data before encryption to prevent data loss if the encryption fails. For example, this can occur if there is insufficient space on the device. ■ **Deleted** - Non-Business related data is deleted. ■ **Untouched** - Non-Business Related data is not encrypted or moved.
Secure format media before encryption	Run a secure format before encrypting the storage device. Select the number of format passes to do before the encryption starts.
Change device name and icon after encryption	When selected, after the device is encrypted, the name of the non-encrypted drive changes to **Non Business Data** and the icon changes to an open lock. When cleared, the name of the non-encrypted drive and the icon do not change after the device is encrypted.

Offline Access Settings

Setting	Description
Password protect media for access in offline mode	Lets users assign a password to access a storage device from a computer that is not connected to an Endpoint Security Management Server. Users can also access the storage device with this password from a non-protected computer
Allow user to recover their password using remote help	Lets user recover passwords using remote help.

Setting	Description
Copy utility to media to enable media access in non-protected environments	Copies the Explorer utility to the storage device. This utility lets users access the device from computers that are not connected to an Endpoint Security Management Server.
Protect media with password for read-only access in offline mode	Lets users assign a different password that gives read-only access to a storage device.
Allow user to change read-only password	Lets users change a previously defined read-only password.

Configuring Encryption Container Settings

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 use

   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**.

Password Constraints for Offline Access

In the Properties of the Offline Access action, click **Configure password constraints** to set the requirements for password used to access encrypted devices.

These Actions define the requirements for user passwords for Media Encryption & Port Protection:

Action	Description
Use Windows password complexity	The standard Windows password requirements are enforced: The password must: ■ Have at least six characters ■ Have characters from at least 3 of these categories: uppercase, lowercase, numeric characters, symbols.
Use custom password complexity	If you select this, select the requirements for which type of characters the password must contain or not contain.

Double-click an action to edit the properties:

Option	Description
Use custom requirements	If you select this, select the requirements for which type of characters the password must contain or not contain: ■ Consecutive identical characters, for example, aa or 33 ■ Require special characters. These can be: `~ = + - _ ( ) ' $ @ , .` ■ Require digits, for example 8 or 4. ■ Require lower case characters, for example g or t. ■ Require upper case characters, for example F or G. ■ Password must not contain user name or full name.
Minimum length of password	Enter the minimum number of characters for a valid password.
Password can be changed only after	Enter the minimum number of days that a password must be valid before the user can change it.
Password expires after	Enter the maximum number of days that a password can be valid before the user must change it.
Number of passwords	Enter the minimum number of password changes needed before a previously used password can be used again.

Media Lockout Settings

You can configure Media Encryption & Port Protection to lock a device after a specified number of unsuccessful login attempts:

- **Temporarily** - If a device is locked temporarily, users can try to authenticate again after a specified time.
- **Permanently** - If the device is locked permanently, it stays locked until an administrator unlocks it.

Select one of these Actions to define if and when user accounts are locked:

Action	Description
Do not lock out storage device upon failed authentication.	Users are not locked out of a device if they try to log on unsuccessfully. This setting is not recommended.
Temporarily lock storage device upon failed authentication attempts	After a configured amount of failed log on attempts (the default is 5), the device is temporarily locked.
Permanently lock storage device upon failed authentication attempts	After a configured amount of failed log on attempts (the default is 10), the device is permanently locked.

Right-click an Action to edit the properties. You can also create custom device Lock actions.

Device Scanning and Authorization Actions

You can configure a Media Encryption & Port Protection rule to require malware and unauthorized file type scans when a storage device is attached. You also can require a user or an administrator to authorize the device. This protection makes sure that all storage devices are malware-free and approved for use on endpoints.

On E80.64 and higher clients, CDs and DVDs (optical media) can also be scanned.

Note - After a media device is authorized:

- If you make changes to the contents of the device in a trusted environment with Media Encryption & Port Protection, the device is not scanned again each time it is inserted.
- If you make changes to the contents of the device in an environment without Media Encryption & Port Protection installed, the device is scanned each time it is inserted into a computer with Media Encryption & Port Protection.

You can select one of these predefined options for a Media Encryption & Port Protection rule:

Action	Description
Require storage devices to be scanned and authorized. Allow self-authorization.	Scan the device when inserted. If this option is selected, users can scan the storage device manually or automatically. If this setting is cleared, users can only insert an authorized device.
Require storage devices to be scanned and authorized. Do not allow self-authorization.	Scan the device when inserted. Specified administrators must authorize the device after a successful scan.
Do not scan storage devices	Storage devices are not scanned when inserted and no authorization is necessary.
New	Create a custom action with different authorization and media scan requirements.

You can configure which file types can or cannot be on storage devices.

To configure which file types can be on storage devices:

1. In a Media Encryption & Port Protection rule, click a device scanning and authorization action and select **Edit Properties**.
2. Click the **Configure unauthorized file types** link.
3. In the **Unauthorized File Types** window, select a **Mode**:

- **Unauthorized** - Configure the file types that are blocked. All other file types are allowed.
- **Authorized** - Configure the file types that are allowed. All other file types are blocked.

The default is unauthorized with all file types allowed.

4. Click **Add** to add file types to the list.
5. Select file types from the **Available Objects** list and click **Add** to move them to the **Selected Objects** list.

   If you selected **Unauthorized** mode, select the file types that are not blocked from storage devices.

   If you selected **Authorized** mode, select the file types that are allowed on storage devices.
6. Optional:
   - Click **New** to create a new file type.
   - Click **Remove** to remove a group from the list.
7. Click **OK**.
8. Click **OK**.

To enable or disable scans for optical media (CDs and DVDs):

1. In a Media Encryption & Port Protection rule, click a device scanning and authorization action and select **Edit Properties**.
2. In the **Device Overrides** area:
   - To disable scans, select **Exclude optical media from scan**.
   - To enable scans, clear **Exclude optical media from scan**.
3. Click **OK**.

Custom Scan and Authorization Actions

You can create custom actions that have different requirements for authorization and the media scan. You can let users connect storage devices without a scan or delete unauthorized file types from the storage device.

To define custom actions:

1. Double-click an action in a rule and select the **New** action.
2. In the **Edit Properties** window, configure these parameters as necessary:

Parameter	Description
Name	Unique action name.
Comments	Optional textual comments.
Scan storage devices and authorize them for access	Select to scan the device when inserted. Clear to skip the scan.
Enable self-authorization	If this option is selected, users can scan the storage device manually or automatically. If this setting is cleared, users can only insert an authorized device.
Automatic media authorization	The device is authorized automatically.
Allow user to delete unauthorized files.	The user can delete unauthorized files detected by the scan. This lets the user or administrator authorize the device after the unauthorized files are deleted.
Manual media authorization	Users or administrator must manually authorize the device.
Allow user to skip media scan	The user can optionally skip the scan when a device is connected to a client.

Log Actions

This setting defines when Media Encryption & Port Protection creates log entries when a storage device is attached to an endpoint computer. You can select one of these predefined log actions:

Action	Description
Do not log security events	Disable **all** log entries.
Log only critical events	Create log entries only for events that are classified as critical.
Log critical and security events	Create log entries only for events that are classified as critical or security events.
Log all events	Create log entries for all events.

You cannot define custom log actions.

This table shows the applicable Media Encryption & Port Protection events and their severity classification.

Event ID	Description	Classification
3	Policy update completed successfully	Low
7	Device authorization successful	Low
8	Device authorization failed	Critical
11	Device access is blocked when attached to the endpoint computer	Critical
15	Encrypted storage created successfully	Low
16	Encrypted storage device removed	Critical
20	Device is attached to an endpoint computer and access is allowed	Security
21	A user follows the Ask User procedure to override a rule	Critical
22	A users does not follow the Ask User procedure to override a rule	Critical
23	A storage device file operation is blocked	Critical

Event ID	Description	Classification
24	A storage device file operation is allowed	Security

You can define different log settings for *"Defining Exceptions for Devices " on page 290*.

Log entries are initially stored on client computers and then uploaded to the server at predefined intervals.

UserCheck Actions

UserCheck for Media Encryption & Port Protection tells users about policy violations and shows them how to prevent unintentional data leakage. When a user tries to do an action that is not allowed by the policy, a message shows that explains the policy.

You can optionally let users write to a storage device even though the policy does not allow them to do so. In this case, users are prompted to give justification for the policy exception. This justification is sent to the security administrator, who can monitor the activity.

You can use the default UserCheck messages or define your own custom messages.

To change an existing UserCheck message:

1. Right-click a UserCheck action, and select **Edit**.
2. For each UserCheck message type, select an option to show a message.

   Clear an option to prevent a message from showing.
3. **Optional**: Click **Configure** to define a custom UserCheck message.
4. **Optional**: Click **Configure** to define a custom **Ask User** message.

To define a custom UserCheck message:

1. Right-click a UserCheck action, and select **Custom**.
2. Enter a unique name for the new action.

   You can optionally add text comments and select a display color.
3. Do steps 2 through 5 in the above procedure as necessary.

Media Encryption Site Actions

Site Actions control when to allow or prevent access to encrypted devices that were encrypted by different Endpoint Security Management Servers. Each Endpoint Security Management Server (known as a Site) has a Universally Unique Identifier (UUID). When you encrypt a storage device on an Endpoint Security client, the Endpoint Security Management Server UUID is written to the device. The Site action can prevent access to devices encrypted on a different Endpoint Security Management Server or from another organization. The Site action is enabled by default.

When a user attaches a storage device, Media Encryption & Port Protection makes sure that the device matches UUID the Endpoint Security Management Server UUID or another trusted Endpoint Security Management Server. If the UUIDs match, the user can enter a password to access the device. If the UUID does not match, access to the device is blocked.

This table shows what occurs when you insert an encrypted device into a client that is connected to an Endpoint Security Management Server the policy allows read- access. The Endpoint Security Management Server that the device was encrypted with is referred to as "the encrypting Endpoint Security Management Server".

The client is connected to:	Action
The encrypting Endpoint Security Management Server	User can access automatically or enter a password for access.
A different trusted Endpoint Security Management Server	User can enter a password for access.
A non-trusted Endpoint Security Management Server	User cannot access the device.

Configuring Media Encryption Site Actions

Media Encryption Site actions are part of the Media Encryption & Port Protection Policy. This predefined action is enabled by default. You can change this action or create your own custom actions.

Action	Description
Allow access to media encrypted at current site only	Media Encryption Site (UUID) verification is enabled. Endpoint Security clients can only access encrypted devices that were encrypted by the same Endpoint Security Management Server. If you add Endpoint Security Management Servers to the table below, they are considered trusted and devices encrypted on those servers are allowed also.

To allow access to devices encrypted on other trusted Endpoint Security Management Servers:

1. Right-click a Media Encryption Site action and select **Edit**.
2. Select **Endpoint client will allow access only to encrypted media that was encrypted by an Endpoint client connected to one of the following management servers**.
3. Click **Add > New**.
4. In the **New Management Server** window, enter:
   - **Name** - A descriptive name for the trusted server.
   - **Comments** - Optionally add free text comments.
   - **Server UUID** - The trusted Endpoint Security Management Server UUID.
5. Click **OK**.

To allow access to devices encrypted on this Endpoint Security Management Server from other Endpoint Security Management Servers:

1. Right-click a Media Encryption Site action and select **Edit**.
2. The **Edit Properties** window opens.
3. Select **Endpoint client will allow access to encrypted media that was encrypted by an endpoint client connected to any management server**.
4. Click **Copy to Clipboard** and then save the current Endpoint Security Management Server UUID to a text file.
5. Add the current Endpoint Security Management Server, using the saved UUID, to the Media Encryption Action to each trusted Endpoint Security Management Server.

To disable Media Encryption sites:

1. Right-click the **Allow access to media encrypted at current site only** action.
2. Select **Edit**.
3. In the **Select Action** field, select **New**.

   This creates a new site action.
4. In the **Policy Action Single Page Form** window, give the policy a different name and description.
5. Click **OK**.

6. Select **Endpoint Client will allow access to encrypted media which was encrypted by an endpoint client connected to any management server**.
7. Click **OK**.

When Media Encryption Sites is disabled, Endpoint Security clients can access storage devices that were encrypted by all Endpoint Security Management Servers.

Global Automatic Access Action

You can select a global action that defines automatic access to encrypted devices. This has an effect on all Media Encryption & Port Protection rules, unless overridden by a different rule or action.

To enable automatic access:

- Make sure that **Removable Media Read Access** actions allow access for the specified users or computers.

  Note - Users cannot access encrypted devices by entering a password if read access is not allowed for that user.

- Select or define an action that allows **Automatic Access** for the logged in user.

Media Encryption & Port Protection comes with these predefined actions:

Action	Description
Encrypted storage devices are fully accessible by all users	All users can read and change all encrypted content.
All users in the organization can read encrypted data, only owners can modify	All users can read encrypted files on storage devices. Only the media owner has can change encrypted content.
Only owners can access encrypted data	Only media owners read and/or change encrypted content.
Access to encrypted data requires password authentication	Users must enter a password to access the device. Automatic access in not allowed.

Custom Automatic Access Action Rules

To create custom action rules:

1. Right-click a Global Automatic Access action and select **Edit**.

   The **Custom Encrypted Media Access Rules** window opens. There are two predefined action rules in this window. You cannot delete these rules or change the media owner or media user. But, you can change the access permissions.

   The two predefined actions are defaults that apply when no other custom action rules override them. The **Any/Media Owner** action rule is first by default and the **Any/Any** action rule is last by default. We recommend that you do not change the position of these rules.

2. Click **Add**.
3. In the **Encrypted Media Owner** field, click the arrow and select one of these options:
   - **Any** - This action applies to any media owner
   - **Choose User/Group/OU from your organization** - Select the applicable user, group or OU that this action applies to
4. In the **Encrypted Media User** field, click the arrow and select one of these options:
   - **Any** - This action applies to any user
   - **Media owner** - The media owner is also defined as the user
   - **Choose User/Group/OU from your organization** - Select the applicable user, group or OU that this action applies to
5. In the **Access Allowed** field, select one of these permissions:
   - **Full Access**
   - **Read Only**
   - **No Automatic Access**

To delete a custom action rule, select the action and click **Remove**. To edit an action, simply select the field in the applicable action and change the parameter.

Anti-Malware

Check Point Anti-Malware protects your network from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers. Use Anti-Malware to centrally manage the detection and treatment of malware on your endpoint computers.

The Endpoint Security Management Server regularly updates Anti-Malware definitions from a Check Point update server.

Prerequisites for Anti-Malware

Before configuring Anti-Malware, you must:

1. **Configure the Endpoint Security Management Server to work with a proxy server**

    a. On the Endpoint Security Management Server, run:

    ```
    cpstop
    ```

    b. Open `$UEPMDIR/engine/conf` and edit the `local.properties` file.

    Note - Delete the # character from the beginning of each row that you edit.

    c. Add these properties:

Property	Example
Proxy server's IP address	`http.proxy.host=<IP address>`
The proxy server's listening port	`http.proxy.port=<port number>`
The username if basic authentication is enabled on the proxy server. Leave it empty if no authentication is required.	`http.proxy.user=<username>`
The password if basic authentication is enabled on the proxy server.	`http.proxy.password=<password>`

    d. Save the `$UEPMDIR/engine/conf/local.properties` file.

e. On the Endpoint Security Management Server, run:

```
cpstart
```

2. **Configure the Firewall Gateway to accept traffic from Anti-Malware signature update servers and Cloud Reputation services**

   After configuring the proxy server, configure the Firewall Gateway to accept the traffic to the Anti-Malware update servers.

   a. In your Firewall Gateway, allow outbound internet connectivity.

   b. In your Firewall Gateway, allow outbound connectivity to the Anti-Malware update server.

3. **Configure the Firewall Gateway to allow the Endpoint Security server to access ports 80 and 443**

   The Endpoint Security server must have access to ports 80 and 443 on the Anti-Malware Signature Update Server to retrieve the latest malware definitions. Make sure that your Firewall Gateway allows this traffic.

4. **Install the Anti-Malware Engine on the Endpoint Security Servers**

   The Endpoint Security Management Server gets the Malware signatures from the central Malware definition server. Endpoint Security clients with the Anti-Malware component get Malware signature updates either from the Endpoint Security Management Server or from their Endpoint Policy Server.

   By default, the Endpoint Security Management Server and the Endpoint Policy Servers do not have the Malware update engine installed. You must install the Malware update engine on:

   - The Endpoint Security Management Server - From SmartEndpoint.
   - Endpoint Policy Servers - By installing a hotfix using CPUSE .

   To Install the Malware update engine on the Endpoint Security Management Server

   a. Open SmartEndpoint

   b. From the **Menu**, select **Tools** > **Anti-Malware Updates**.

   c. Click **Download and install engine**.

Configuring Anti-Malware Policy Rules

For each action in a rule, select an option, which defines the action behavior. You can select a predefined **Action** option or select **New** to define a custom action.

Right-click an **Action** and select **Edit** or **Edit Shared Action** to change the action behavior.

Changes to policy rules are enforced only after you install the policy.

Note that exclusions that you configure in one action apply to all Anti-Malware scans.

Scan All Files on Access

By default, all file are scanned when they are opened or used.

You can configure **Trusted Processes** as exceptions. When a trusted process accesses a file, the file is not scanned. Exclude a process only if you fully trust it and are sure it is not malware.

You can also select or clear these options:

- **Detect Unusual Activity** - Use behavior detection methods to protect computers from new threats whose information has not been added to the databases yet. It does not monitor trusted processes.
- **Enable Cloud Reputation Services For Files, Web Resources, and Processes** - Use cloud technologies to improve precision of scanning and monitoring functions. If you enable or disable this setting, it takes affect after the client computer restarts.
    - **Connection Timeout** - Change the maximum time to get a response from Reputation Services (in milliseconds).

      Note - If you decrease this value, it can improve the performance of the Anti-Malware component but reduces security, as clients might not get a reputation status that shows an item to be zero-day malware.
- **Enable Web Protection** - Prevents access to suspicious sites and execution of malicious scripts. Scans files, and packed executables transferred over HTTP, and alerts users if malicious content is found.
- **Mail Protection** - Enable or disable scans of email messages when they are passed as files across the file system.

To configure trusted processes:

1. In the **Properties** of the **Scan all files on Access** Action, click **Add**.
2. In the **Trusted Processes** window, enter the fully qualified path or an environment variable for the trusted executable file. For example:

- `C:\Program Files\MyTrustedDirectory\MyTrustedProgram.exe`
- `%programdata%\MyTrustedProgram.exe`

3. Click **OK**.

   The trusted program shows in the **Trusted Processes** list.

Malware Signature Updates

Anti-Malware gets malware signature updates at regular intervals to make sure that it can scan for the newest threats.

These actions define the frequency of the signature updates and the source.

Action	Description
Check for malware signature updates every 4 hours	Signature updates occur every 4 hours from the Endpoint Policy Server and Check Point server.
Check for malware signature updates every 2 hours	Signature updates occur every 2 hours from the Endpoint Policy Server and Check Point server.

Double-click an **Action** to edit the **Properties**.

You can change these settings:

- **Check for updates every** - Frequency, in hours, between client requests for malware signatures and scanning for engine updates.
- **Signature update will fail after** - The connection timeout, after which the update source is considered unavailable.
- **Update Signatures From** - The server or servers that the client gets updates from.
  - **Signature Source:**
    - **External Check Point Signatures Server** - Get updates from a dedicated, external Check Point server through the internet.
    - **Local Endpoint Servers** - Get updates from the Endpoint Security Management Server or configured Endpoint Policy Server.
    - **Other External source** - Get updates from an external source through the internet. Enter the URL.
    - **Shared Signature Source** - Get updates from a shared location on an Endpoint Security client that acts as a *Shared Signature Server*. This makes it possible to protect non-persistent virtual desktops in Virtual Desktop Infrastructure (VDI) environments. Each non-persistent virtual desktop runs an Endpoint Security Client, and gets the Anti-Malware signatures from a shared folder on the Shared Signature Server that is a persistent virtual machine. To learn more, see *"Shared Signature Server for Anti-Malware" on page 317*
  - **If first update fails** - Set a fallback update source to use if the selected update source fails. Select a different option than the first signature source.

- **If second update fails** - Set a second fallback update source to use if the other sources fail.

Note - If only **Update from Local Endpoint Servers** is selected, clients that are disconnected from an Endpoint Security server cannot get updates.

Anti-Ransomware Files

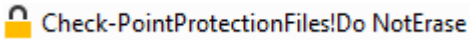
Anti-Ransomware creates honeypot files on client computers. It stops the attack immediately after it detects that the ransomware modified the files.

The Anti-Ransomware creates the honeypot files in these folders:

- `C:\Users\Public\Music`
- `C:\Users\<User>\Music (MyMusic)`
- `C:\Users\Public\Documents`
- `C:\Users\<User>\Documents (MyDocuments)`
- `C:\Users\Public\Videos`
- `C:\Users\<User>\Videos (MyVideos)`
- `C:\Users\Public\Pictures`
- `C:\Users\<User>\Pictures (MyPictures)`
- `C:\Program Files (x86)`
- `C:\ProgramData`
- `C:\Users\<User>\AppData\Roaming`
- `C:\Users\<User>\AppData\Local`
- `C:\Users\<User>\Downloads`

You can identify these folders by the lock icon that is associated with the name of the folder.

For example:



The file names include these strings, or similar:

- `CP`
- `CheckPoint`
- `Check Point`
- `Check-Point`
- `Sandblast Agent`

- `Sandblast Zero-Day`
- `Endpoint`

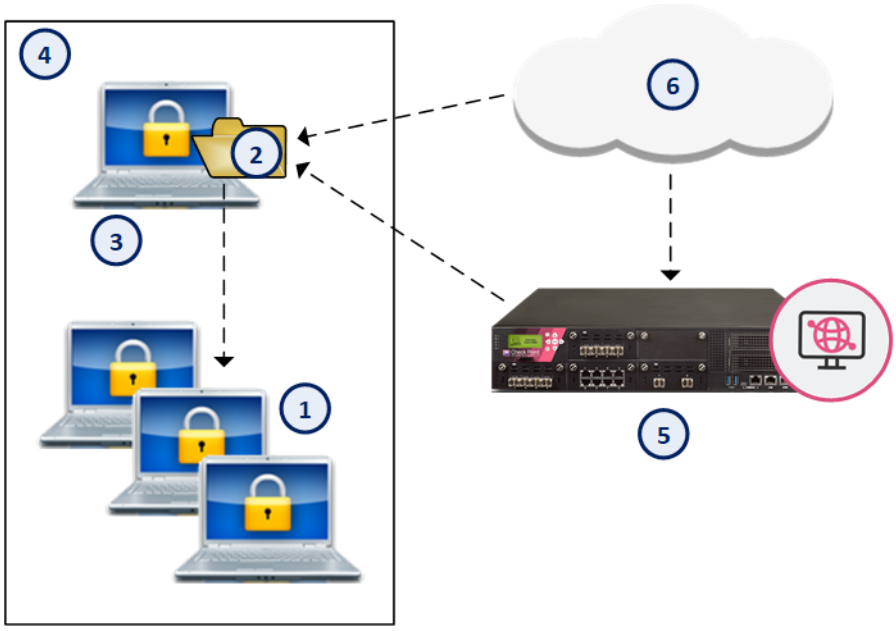
You can open and look at the files. They are real documents, images, videos, and music.

If a file is deleted, it is automatically recreated after the next system boot.

Shared Signature Server for Anti-Malware

Endpoint computers (1) can get the latest Anti-Malware signatures from a shared location (2) on an Endpoint Security client computer (3) that acts as a *Shared Signature Server*. This capability makes it possible to protect non-persistent virtual desktops (1) in a Virtual Desktop Infrastructure (VDI) environment (4). Each non-persistent virtual desktop runs an Endpoint Security Client, and gets the Anti-Malware signatures from a shared folder (2) on the Shared Signature Server (3) that is a persistent virtual machine.

The numbers in the text refer to the diagram:



The Shared Signature Server (3) gets the latest signatures from one of these sources:

- An Endpoint Security Management Server or Endpoint Policy Server (5).
- Over the Internet from the Check Point Signature server (6). The domain name of that server is `kav8.checkpoint.com`.

The Shared Signature Server must run on a persistent virtual machine, preferably on the same VDI host storage (4) as the clients.

In SmartEndpoint you need to configure two Anti-Malware policy rules. One rule for the Shared Signature Server and one rule for the non-persistent virtual desktops.

Note - Here you can learn how to use SmartEndpoint to configure the Shared Signature Server for Anti-Malware. To learn how to set up all the other requirements for Endpoint Security in VDI environments, see the *Endpoint Security VDI Administration Guide*.

Configuring the Shared Signature Server and Clients

Configure one Computer Group for the Shared Signature Server, and one Computer Group for the clients. Then, define one Anti-Malware policy rule for the Shared Signature Server, and one rule for the clients.

1. Define a Computer Group that contains the Endpoint Security computer that is the Shared Signature Server

1. In the **Users and Computers** tree, click **Global Actions** > **New Virtual Group**.
2. In the **New Virtual Group** window:
   - Enter a name for the group.
   - Optional: Enter a **Comment**.
   - Select **Computer Group**.
3. Click **Next**.
4. In the **Select Entities** window, select the Endpoint Security computer that is the Shared Signature ServerS.
5. Click **Finish**.

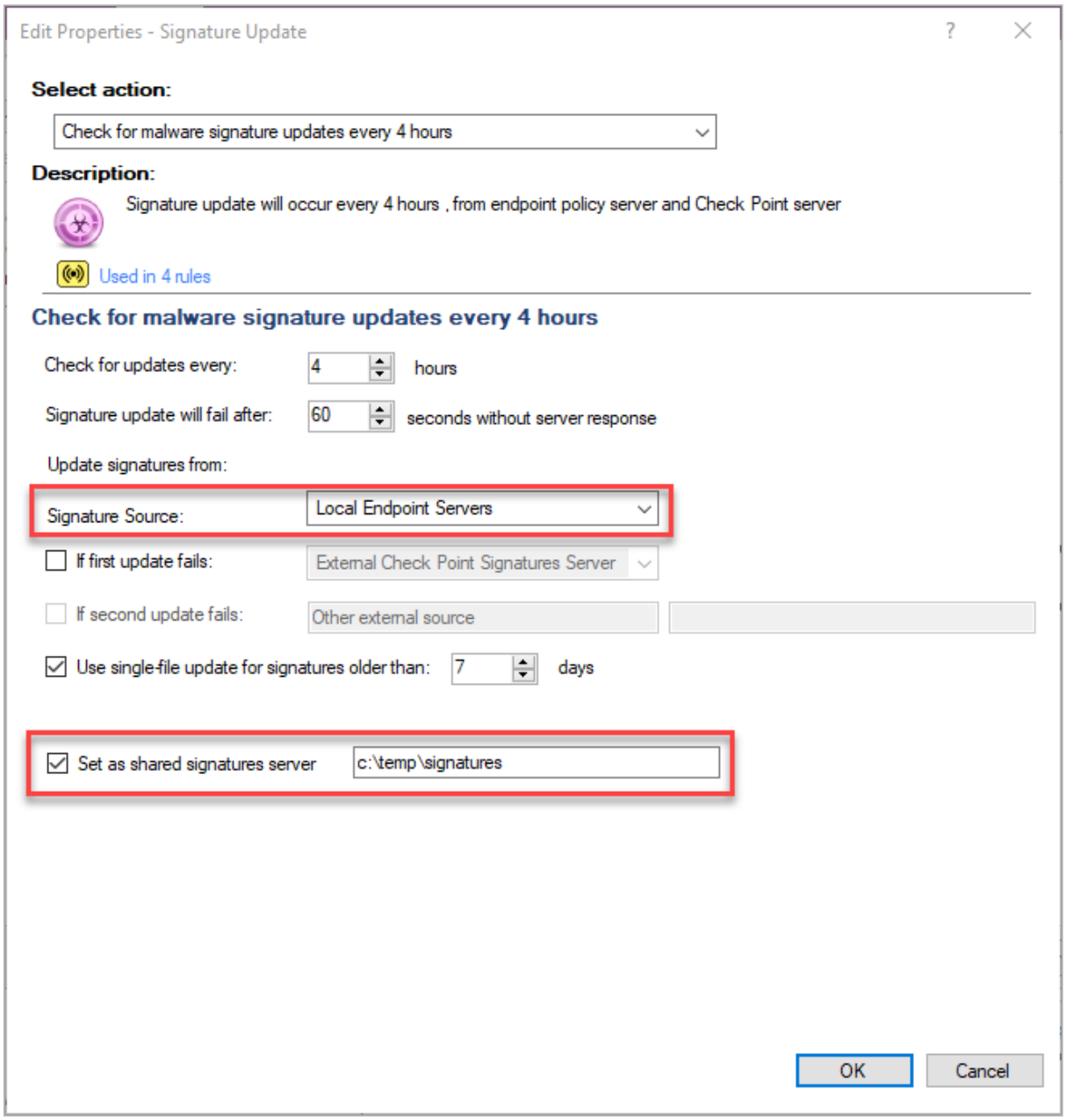
2. Define a Computer Group that contains all the Endpoint Security clients on non-persistent desktops

1. Create a new Virtual Group of type **Computers Group**.
2. In the **Select Entities** window, select all the non-persistant virtual desktops with Endpoint Security, that are created with the Golden Image.

3. Create a rule for the Shared Signature Server

1. In the Anti-Malware policy, right-click the rule **Default Anti-Malware settings for the entire organization** and select **Clone Rule**.
2. The **Create Rule Wizard** opens.
3. Click **Next**.
4. In the **Select Entities** page, select the Computer Group of the Shared Signature Server.
5. Click **Next**.

6. In the **Change Rule Action** page, click **Signature Update** and select **Edit Shared Action**.
7. In **Signature Source**, select one of the following:
   - **Local Endpoint Servers** - Get updates from the Endpoint Security Management Server or an Endpoint Policy Server.
   - **Other External source** - Get updates over the Internet. For example, to get updates from the Check Point Signature server, enter `kav8.checkpoint.com`
8. In **Set as Shared Signature Server**, enter the path of the shared folder, for example `C:\temp\Signatures`

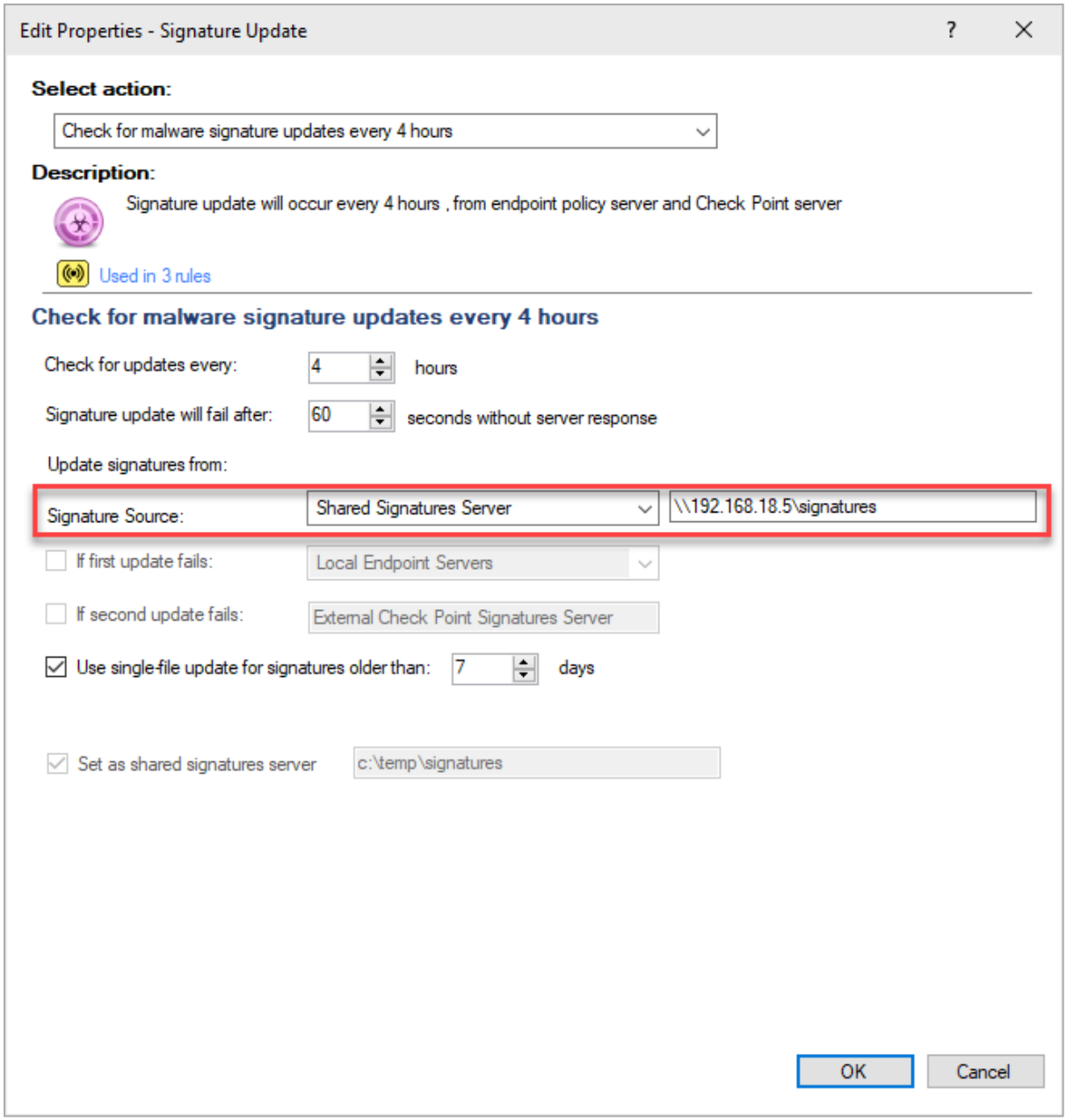


9. Click **Next**.

10. In the **Name and comment** page, enter a descriptive **Name** for the rule.
11. Click **Finish**.

4. Create a rule for the Endpoint Security clients on non-persistent desktops

1. Right-click the rule **Default Anti-Malware settings for the entire organization** and select **Clone Rule**.
2. The **Create Rule Wizard** opens.
3. Click **Next**
4. In the **Select Entities** page, select the Computer Group of the clients on non-persistent desktops.
5. Click **Next**.
6. In the **Change Rule Action** page, click **Signature Update** and select **Edit Shared Action**.
7. In **Signature Source**, select **Shared Signature Server**.
8. Enter the shared location of the signatures on the server, in the format `\\<client name or IP address>\folder`
   For example `\\192.168.18.5\Signatures`



9. Click **Next**.
10. In the **Name and comment** page, enter a descriptive **Name** for the rule.
11. Click **Finish**.

5. Install the Anti-Malware policy

1. In the **Policy** tab, go to the Policy Toolbar.
2. Click Install

Performing Periodic Anti-Malware Scans

Anti-Malware scans computers for malware at regular intervals to make sure that suspicious files are treated, quarantined, or deleted.

Choose one of the **Select Action** options to define the frequency of the scans.

Action	Description
Perform periodic anti-malware scan every day	A scheduled scan occurs every day at the time shown in the Properties.
Perform periodic anti-malware scan every week	A scheduled scan occurs every week at the day and time shown in the Properties.
Perform periodic anti-malware scan every month	A scheduled scan occurs every month at the date and time shown in the Properties.

Double-click an Action to edit the **Properties**.

Select the day and time of day that the scan occurs.

Optional: Select **Randomize scan time** to make sure that not all computers do a scan for malware at the same time. This makes sure that network performance is not affected by many simultaneous scans. In **Start scan between**, specify the time range during which the scan can start.

The targets of the scan are defined in the action: *"Periodic Scan Options" on page 323*.

Periodic Scan Options

These Actions define which components of computers are scanned during the scheduled malware scans.

Action	Description
Periodically scan system critical areas only	The scheduled scan scans system critical areas, for example: the operating system, processes, and memory. These are the targets of most malicious programs.
Periodically scan local hard-drives	The scheduled scan scans system critical areas and local drives.
Periodically scan local and removable drives	The scheduled scan scans system critical areas and local and removable drives.

Double-click an Action to edit the Properties.

You can change:

- The exact scan targets.
- Files or folders that are excluded from scans.

  Note - Files that a user scans with *Contextual scan* are always scanned, even if they are excluded by type, or size, or are in this list of excluded files and folders. A contextual scan is a scan that the user runs from the right-click menu of the file that the user wants to scan: The user does a right-click on a file and selects **Scan with Check Point Anti-Malware**.

  - **Skip archives and non executables** - When selected, these types of files are not scanned.
  - **Do not scan files larger than** - Select the maximum size of files to be scanned. This option applies to On Demand scans and Scheduled scans. It does not apply to On Access scans.
  - **Configure files and folders exclusions** - Click to configure specified file or extensions to exclude.

Exclude Files and Folders from Scan

You can exclude the contents of trusted directories or files and specified trusted program executables from the Anti-Malware schedules scan. You can also exclude all files of a specified file extension.

For example, you might exclude these types of directories or programs from the scan:

- The directory or program is located in a Trusted Zone
- The directory or program is a low risk target for viruses
- Scanning has an adverse effect on computer performance

Excluding a folder prevents the Anti-Malware scanner from examining the folder contents. Excluding a process lets the specified, trusted executable run without being monitored by Anti-Malware. Exclude a process only if you fully trust it and are sure it is not malware.

Excluded items are not scanned during full computer, scheduled, and on access scans. They are not excluded from scans initiated by users with a right-click > **Scan with Check Point Anti-Malware**.

Notes -

- All directory paths must end with a backslash, for example: `driveletter:\folder\.`
  Filenames do not end with a backslash.
- You cannot use environment variables to exclude folders and file paths.

To configure a list of file paths that are excluded from scans:

1. Right-click the **Periodically scan** action and select **Edit Properties**.
2. In the **Properties** window, click the **Configure files and folders exclusions** link.
3. In the **New File Path Exclusion Properties** window, click **Add** and enter:
   - The fully qualified path to a file, file type, or directory (including its subdirectories) to be excluded from the malware scan.
   - The fully qualified path to a trusted executable to be excluded from malware monitoring.
4. In the **Path Exclusions** window, click **Browse** and go to the trusted directory. Alternatively, you can:
   - Enter a directory path.
     Example: `C\Program Files\MyTrustedDirectory\`
   - Enter a specific file
     Example: `C:\Program Files\excludeMe.txt`
   - Enter a file type
     Example: `*.txt`
5. Click **OK**.

   The trusted directory shows in the **Scan exclusions** list.

Scan Optimization

The scan optimization options let you do malware scan quickly and with less impact on performance and system resources.

Scan priority is lower than other running processes by default.

The options are:

Do not optimize malware scan - Scan optimization is disabled.

Optimize malware scan:

- **Perform scan optimizations** - Optimize the scan by storing file checksums and NTFS file system data during the first scan. NTFS cluster size, file name, and folder structure are cached. During subsequent scans, only new files or files whose checksum, file size, name, or structure has changed are scanned.

Malware Treatment

The malware treatment options let you choose what happens to malware that is detected on a client computer.

Double-click an Action to edit the **Properties**.

You can change the settings for malware and riskware. The options are:

- **Malware Treatment** - Malware is software that is definitely dangerous.
  - **Quarantine file if cure failed** - If Endpoint Security cannot repair the file, it is deleted and put in a secure location from where it can be restored if necessary.
  - **Delete file if cure failed** - If Endpoint Security cannot repair the file, it is deleted.
- **Riskware Treatment** - Riskware is legal software that might be dangerous.
  - **Treat as malware** - Use the option selected for Malware.
  - **Skip file** - Do not treat riskware files.

Excluding Infections by Name

You can create a list of infections (by name) that will get different treatment than the selections above. Use an exception to allow a file that was detected as a threat in your organization, but was a false positive or riskware (software that can have both legitimate and malicious usage). For example, RAdmin might be detected as a threat but you want to allow it.

Contextual scans are done even if the file is in the *Exclude Infections by Name* list. A contextual scan is a scan that the user runs from the right-click menu of the file that the user wants to scan: The user does a right-click on a file and selects **Scan with Check Point Anti-Malware**.

You can get the virus names of threats detected in your organization from one of these sources:

- In SmartEndpoint > **Users and Computers**, select a computer and click **Anti-Malware**. The list of infections for that computer show.
- The **Top Infections** report.
- Anti-Malware infection logs in SmartLog

To create a list of exceptions for malware treatment:

1. In the **Edit Properties - Malware Treatment** window, click **Exclude infections by name**.
2. Click **Add** to add infections to the list.
3. Enter the name of the infection.

4. Click **OK**.
5. Click **OK**.

Submitting Malware and False Detections

Reporting suspected malware or false detections to Check Point helps to improve the security and protection of all Internet users.

If you think that you have malware in your organization that was not detected by Anti-Malware, contact Check Point Technical Support. If Anti-Malware mistakenly identifies a file as malware, contact Check Point Technical Support.

Harmony Endpoint Anti-Ransomware, Behavioral Guard and Forensics

The Harmony Endpoint Forensics and Anti-Ransomware component monitors file operations, processes, and network activity for suspicious behavior. It also analyzes attacks detected by other client components or the Check Point Security Gateway. It applies Remediation to malicious files.

Anti-Ransomware constantly monitors files and processes for unusual activity. Before a Ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

All details of attacks are organized in the Forensics Analysis Report.

For example, if Harmony Endpoint Anti-Bot detects a malicious URL, it notifies Forensics through internal communication. Forensics starts a complete investigation and generates a Forensics Analysis Report.

You can also configure the Forensics component to analyze incidents that are detected by a third party Anti-Malware solution.

Configure the settings in the **Harmony Endpoint Forensics and Anti-Ransomware** rule of in the SmartEndpoint **Policy** tab.

If Endpoint Security servers do not have internet connectivity, Forensics information is stored and sent for evaluation immediately when a server connects to the internet.

Anti-Ransomware Files

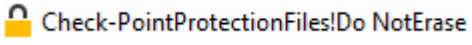
Anti-Ransomware creates honeypot files on client computers. It stops the attack immediately after it detects that the ransomware modified the files.

The Anti-Ransomware creates the honeypot files in these folders:

- `C:\Users\Public\Music`
- `C:\Users\<User>\Music (MyMusic)`
- `C:\Users\Public\Documents`
- `C:\Users\<User>\Documents (MyDocuments)`
- `C:\Users\Public\Videos`
- `C:\Users\<User>\Videos (MyVideos)`
- `C:\Users\Public\Pictures`
- `C:\Users\<User>\Pictures (MyPictures)`
- `C:\Program Files (x86)`
- `C:\ProgramData`
- `C:\Users\<User>\AppData\Roaming`
- `C:\Users\<User>\AppData\Local`
- `C:\Users\<User>\Downloads`

You can identify these folders by the lock icon that is associated with the name of the folder.

For example:



The file names include these strings, or similar:

- `CP`
- `CheckPoint`
- `Check Point`
- `Check-Point`
- `Sandblast Agent`
- `Sandblast Zero-Day`
- `Endpoint`

You can open and look at the files. They are real documents, images, videos, and music.

If a file is deleted, it is automatically recreated after the next system boot.

Configuring Forensics and Anti-Ransomware Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

The **Default Forensics settings** rule applies to the **Entire Organization**. You can edit the default rule, but you cannot delete it.

Automatic Threat Analysis Settings

Define the automatic threat analysis settings in the **Triggers and Automatic Response** Action.

The automatic options are:

- **Automatically analyze threats** - Analyze incidents based on Check Point's recommended triggers (default).
- **Automatically analyze and remediate infections** - Analyze incidents based on Check Point's recommended triggers and apply Remediation automatically.
- **Do not analyze threats** - Automatic Forensics analysis is turned off.

You can edit the selections manually to define when these processes occur.

The confidence level is how sure Endpoint Security is that a file is malicious. High confidence means that it is almost certain that a file is malicious. Medium confidence means that it is very likely that a file is malicious.

- **Forensics Analysis** - When Forensics analysis occurs.
- **File Quarantine** - When files are quarantined for Threat Emulation and Anti-Bot.
- **Machine Quarantine** - When machines are quarantined. If a computer is quarantined, the Firewall restricts network access.
- **Attack Remediation** - When Remediation occurs for components that are part of an attack.

To granularly edit which type of events trigger a Forensics response:

1. In a Harmony Endpoint Forensics and Remediation rule, right-click the **Automatic Threat Analysis** Action and select **Edit Shared Action**.
2. Click **Override confidence level per specific event**.

You can override the settings of the rule for up to five different events.

The Triggers include:

- Events detected by Endpoint Security components: Anti-Bot, Threat Emulation, Anti-Malware
- Events detected by Network components: Anti-Bot, Threat Emulation, Anti-Malware, URL Filtering

Configuring Network Blades for Forensics Triggers and Remediation

To make triggers and Remediation work for events detected by Network Threat Prevention components, you must configure Security Gateway policy for the Threat Prevention components: Anti-Bot, Anti-Virus, and Threat Emulation.

Each component must be enabled and have Protection settings of **Prevent** or **Ask**, which include UserCheck.

Best practice is to use the **Threat Prevention Recommended Profile** (default) that includes all required settings.

Monitoring and Exclusions

Define which processes are monitored by the Forensics component.

In the default monitoring settings, processes with certificates from some trusted companies are excluded.

You can **Add**, **Edit**, and **Remove** exclusions from the list.

To exclude a process from monitoring:

1. From a Harmony Endpoint Forensics and Anti-Ransomware rule in the **Policy**, right-click the **Monitoring and Exclusions** action and select **Edit Shared Action**.
2. Click **Add exclusion**.
3. In the window that opens select:
   - **Process** - To exclude an executable. You can also include Certificate information.
     - In **Process name**, enter the name of the executable.
     - Optional: Enter more information in the fields shown **Signer** is the company that signs the certificate. The more information you enter, the more specified the exclusion will be.
   - **Certificate** - To exclude processes based on the company that signs the certificate, for example, Google.
     - In **Certificate Data**, enter a name of company that signs certificates, or browse to add a certificate file.
4. Click **OK**.
5. The exclusion is added to the Exclusions list.

Disk Space for Forensics

By default Forensics uses up to 1 GB of disk space on the client computer for data. You can configure more space for Forensics storage, but not less.

After the threshold is reached, the oldest data is deleted.

Change the **Maximum Forensics Database** size in the **Disk Usage** area of the **Monitoring and Exclusions** Action.

You can configure more settings related to space usage in Database Tool (GuiDBEdit Tool) (see sk13009) or dbedit (see sk13301).

Important - Do NOT use these tools unless instructed by Check Point Support or R&D. Incorrect use may corrupt settings in the management database.

Quarantine Settings and Attack Remediation

Define what happens to the components of an attack that is detected by Forensics. When files are quarantined, they are deleted and put in a secure location from which they can be restored, if necessary.

The automatic options are:

- **Quarantine all attack elements** - All components of the attack are quarantined.
- **Quarantine only files with known malicious reputation** - If a file is not known as malicious, it is not quarantined.

You can manually edit the treatment for each category of file: **Malicious**, **suspicious**, or **unknown**. For each category, you can select:

- **Quarantine** - Files are deleted and put in a secure location from which they can be restored, if necessary.
- **Delete** - Files are permanently deleted.
- **Backup** - Delete the file and create an accessible duplicate.
- **None** - No action is taken.

Trusted Files are those defined as trusted by the Check Point Reputation Service. The Remediation options for **Trusted Files** are:

- **Terminate** - Stop the suspicious process.
- **Ignore** - Do not terminate processes. Activity is monitored.

File Quarantine Settings

Define the settings for files that are quarantined.

In the Default File Quarantine Settings, files are kept in quarantine for 90 days and users can permanently delete items from quarantine.

You can edit the Quarantine settings:

- Click **Add exclusion** to exclude a file or process from quarantine. You can define an exclusion by many different criteria. Criteria include: File extension, certificate data, MD5 hash, and SHA1 hash. Add more information to make the exclusion very specific and less information to make it broad.
- **Quarantine folder name** - Select the quarantine location on client computers.
- **Copy quarantine files to a central location** - Enter a central location that quarantined files from client computers are copied to.
- **Allow users to delete items from quarantine** - When selected, users can permanently delete items from the quarantine file on their computers.
- **Allow users to restore items from quarantine** - When selected, users can restore items from the quarantine file on their computers.

Anti-Ransomware Backup Settings

When Anti-Ransomware is enabled, it constantly monitors files and processes for unusual activity. Before a Ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

Define settings for Anti-Ransomware backup and restoration.

General Anti-Ransomware Settings

- **Enable Anti-Ransomware** - This is selected by default. To disable Anti-Ransomware, clear it.
- **Automatic restore and remediate** - When selected, Anti-Ransomware automatically starts Remediation after a Ransomware attack. It deletes files created by the attack and restores the original files.

  When this is not selected, users must start the restoration from the client computer. See *"Manual Anti-Ransomware Restoration" on the next page*.

  - **Restore to selected location** - By default, files are restored to their original location. To restore files to a different location, click **Choose location**. Each time files are automatically restored, they will be put in this configured location.

Backup Settings

Anti-Ransomware automatically backs up files before they are affected by a Ransomware attack. You can add files, processes, and certificates to the exclusion list to exclude them from backups.

- **Anti-Ransomware Maximum backup size on disk** - Set the maximum amount of storage for Anti-Ransomware backups. Best practice is to allow 1 GB.
- **Backup Time Interval** - Within this time interval, each file is only backed up one time, even if it is changed multiple times.
- **Change default file types to be backed up** - Click this to see a list of file types that are included in the Anti-Ransomware backup files. You can add or remove file types from the list and change the **Maximum Size** of files that are backed up.

To add exclusions from Anti-Ransomware backups:

1. From a Harmony Endpoint Forensics and Anti-Ransomware rule in the **Policy**, right-click the **Anti-Ransomware Backup Settings** action and select **Edit Shared Action**.
2. Click **Add exclusion**.
3. In the window that opens select **Folder**, **Process**, or **Certificate**.

- **Folder** - To exclude all files in a folder, enter the Folder Name or browse to it.
  - Optional: Select **Include all sub folders** to exclude all files contained in all sub folders.
- **Process** - To exclude an executable. You can also include Certificate information.
  - In **Process name**, enter the name of the executable.
  - Optional: Enter more information in the fields shown **Signer** is the company that signs the certificate. The more information you enter, the more specified the exclusion will be.
- **Certificate** - To exclude processes based on the company that signs the certificate, for example, Google.
  - In **Certificate Data**, enter a name of company that signs certificates, or browse to add a certificate file.

4. Click **OK**.
5. The exclusion is added to the Exclusions list.

Manual Anti-Ransomware Restoration

If you select **Automatic restore and remediate** in the **Anti-Ransomware Backup Settings** Action, Anti-Ransomware automatically starts Remediation after a Ransomware attack.

If you do NOT select **Automatic restore and remediate**, end-users must start restoration manually on the client computer after a Ransomware attack.

Best practice is to guide users through the process and instruct them what to select when there is more than one option.

Anti-Ransomware Restoration

In the Harmony Endpoint Forensics Analysis Report (see *"Forensics" on page 346*), you can see details of which files restored and deleted during the restoration.

- See which files were restored in the **Business Impact** section.
- See which files were deleted in the **Remediation** section.

To run Anti-Ransomware restoration from a Windows client computer:

1. Right-click the Endpoint Security icon in the taskbar notification area and select **Display Overview**.

   The **Endpoint Security Main Page** opens.
2. Click **Forensics and Anti-Ransomware** .
3. In the **Analyzed cases** table, click **Restore Files** in the row of the relevant incident.

The **Anti-Ransomware Restoration** windows open.

4. Click **Restore** to start the restoration process.

   If you see a note that the files were already restored, click **Cancel**. It is not necessary to restore the files again.

5. In the **Restore Step 1 of 2** window:

   a. Select the location to place the restored files:

      - **Restore files to the original location** (default)
      - **Restore to selected location** - If you select this, you are prompted to select the location.

   b. **Delete files created by the attack, including encrypted files** - This is selected by default. Clear it if you do not want to delete the files.

   c. Click **Next**.

6. In the **Restore Step 2 of 2** window, click **Restore** to start the process.

   The Endpoint Security Restoration window opens and shows the files that were restored and where they are located.

7. Click **Close**.

Integration with Third Party Anti-Virus Vendors

Forensics can use information from the Windows Event Log to monitor and analyze malware events from third party anti-virus vendors. Based on the Windows Event Log, Forensics can analyze attacks, terminate processes, delete or quarantine files, and do other attack Remediation.

You can enable or disable third party integration in SmartEndpoint, from the **Automatic Threat Analysis** action. This works with most common vendors without manual configuration.

Note - Some third party vendors do not automatically send information to the Windows Event Log. To use third party vendor integration, make sure that your vendor is configured to send information to the Windows Event Log.
Events are detected when the client is online or offline.

Supported Third Party Anti-Virus Vendors

- Windows Defender (English)
- Symantec Endpoint Protection (English)
- F-Secure Anti-Virus (English)
- Kaspersky (English, Russian)
- ESET Smart Security (English)
- ESET NOD32 Antivirus (English)
- ESET Endpoint Antivirus (English)
- Cylance (English)
- McAfee Endpoint Security (English, French)
- Trend Micro (English)

Enabling or Disabling Forensics Third Party Anti-Virus Vendor Integration

To enable or disable Forensics Third Party Anti-Virus Vendor integration:

1. In a Harmony Endpoint Forensics and Remediation rule, right-click the **Automatic Threat Analysis** Action and select **Edit Shared Action**.
2. In the bottom of the window, click **Override confidence level per specific event**.

   The **Confidence level for automatic response** window opens.
3. In the **Additional Events** area, in the **Third party** row under **Forensics Analysis** -

- Select **Always** to enable Third Party Anti-Virus Vendor integration.
- Select **Never** to disable it.

4. Click **OK**.
5. To test the Forensics Third Party Anti-Virus integration:
   a. Create an eicar test file on your device.
   b. After a while, the Forensics analysis initiates.

      You can view the report in your Endpoint Security Client:

For troubleshooting, see sk116024.

Manual Analysis with CLI

You can configure the Forensics component to analyze incidents that are detected by a third party Anti-Malware solution. To use this, after an incident is triggered you can run analysis manually on the client computer or use a dedicated tool.

To run analysis manually on a client computer with CLI:

Use the command:
`C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe <Type>:<Malicious resource> [options]`

Parameter	Description
<Type>	The type of <malicious>: URL, File, MD5, IP [Mandatory]
<Malicious>	The resource description (for example URL). [Mandatory] **Note** - File description can be full path or just file name.
-r, -Remediation	Remediate malicious, suspicious, unknown processes based on policy configuration. [Optional]
-q, -quarantine	Enter the machine to restricted mode based on policy configuration. [Optional]
-id {GUID}	Set ID to incident. The format of the id is GUID. [Optional]
-b, -backup {Directory}	Backup Forensics Database to local file. [Optional]
-h, -help	Open help manual. [Optional]

Examples:

1. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe file:c:\test\test.doc url:www.test.com -r`
2. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe file:test.doc -r -q`
3. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe ip:170.12.1.180 file:test.doc`

4. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe HYPERLINK "url:www.Malicious.com" md5:10010010010010010010010010010 -q -b c:\ backupToFile.txt`
5. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe -b c:\backupToFile.txt`

Notes:

1. All combination between optional parameters are allowed, the order is not important.
2. Backup option does not require Mandatory parameters (example 5).

Manual Analysis with Push Operations

You can trigger incident analysis for a client on a one-time basis with Push Operations. You can run the Push Operations from SmartEndpoint or from the CLI. The analysis occurs without the need to install policy.

To use Forensics Push Operations from SmartEndpoint:

1. In SmartEndpoint, right-click on a computer object and select **Forensics**.
2. Select an option:
   - **Analyze by URL** - Enter the URL to inspect.

     Optional - Enter data to search for an incident that occurred.
   - **Analyze by process or file** - Enter the full path to the file.

     Optional - Enter data to search for an incident that occurred.
3. Click **OK**.

   The Forensics analysis runs on the users' computer.

To use Forensics Push Operations from the Endpoint Security Management Server CLI:

For complete information about a dedicated tool and integration with third party Anti-Malware solutions, see sk105122.

Run the `$UEPMDIR/system/utils/EfrPushOperation.sh` script on a computer, OU, or group.

Usage:

```
EfrPushOperation {-name <node_name> | -fqdn <node_FQDN> | -dn
<node_DN>} {-url <URL> |-file <file>} [-i <start_time> [-r
<range>]] [-a <activity_event>] [-c <case_analysis_event>] -u
<username> -p <password>
```

Parameters:

Parameter	Description
`-name <node_name>`	The requested node name as appears in SmartEndpoint
`-fqdn <node_FQDN>`	The requested node FQDN name (for example, `device1@mycompany.com`)

Parameter	Description
`-dn <node_DN>`	The requested node distinguished name (for example, `CN=device1,OU=Computers,DC=mycompany,DC=com`)
`-url <URL>`	Analyze by URL
`-file <file>`	Analyze by file or process
`-i <start_time>`	Incident start time (date and time)
`-r <range>`	Time range (before and after start time) in minutes
`-a <activity_event>`	'`f`' if detailed activity logs should not be generated, default is '`t`'
`-c <case_analysis_event>`	'`f`' if case analysis report should not be generated, default is '`t`'
`-u <username>`	Security Management Server username (case-sensitive)
`-p <password>`	Security Management Server password (case-sensitive)

Forensics

Harmony Endpoint Forensics analyzes attacks detected by other detection features like Anti-Ransomware or Behavioral Guard, the Check Point Security Gateway and some third party security products. On detection of a malicious event or file, Forensics is informed and a Forensics analysis is automatically initiated. After the analysis is completed, the entire attack sequence is then presented as a Forensics Analysis Report.

The Forensics Analysis Report provides full information on attacks and suspicious behavior with an easy interface. The report includes:

- **Entry Point** - How did the suspicious file enter your system?
- **Business Impact** - Which files were affected and what was done to them?
- **Remediation** - Which files were treated and what is their status?
- **Suspicious Activity** - What unusual behavior occurred that is a result of the attack?
- **Incident Details** - A complete visual picture of the paths of the attack in your system.

Use the Forensics Analysis Report to prevent future attacks and to make sure that all affected files and processes work correctly.

Opening Forensics Analysis Reports

The Forensics Analysis Report opens in your internet browser.

To open a Forensics Analysis Report for an incident:

- **SmartLog** - From the Log Details of a Forensics, Threat Emulation, or Anti-Bot log, under **Forensics**, click **Report**.
- **SmartEvent** - From the Summary of a Forensics, Threat Emulation, or Anti-Bot log, under **Actions**, click **Open Forensics Report**.
- **Endpoint Security Client GUI** - From the Client Overview, open the **Forensics** component and click the **Incident ID** in the incident table.

Harmony Endpoint Dynamic Updates

Harmony Endpoint dynamic updates enable stronger security for endpoints, with regular updates to Harmony Endpoint files. This keeps clients protected from the latest threats.

By default, the Threat Emulation component runs the `EPNetUpdate.exe` process every 6 hours to get updates and update relevant files.

If necessary, you can disable the dynamic updates in Database Tool (GuiDBEdit Tool).

To enable or disable Harmony Endpoint dynamic updates:

1. Close all SmartConsole windows.
2. Connect with Database Tool (GuiDBEdit Tool) (see sk13009) to Endpoint Security Management Server.
3. Search for: **enable_efr_updatability**
4. Right-click and select **Edit**.
5. To change the value:
   - **true** - enabled (default)
   - **false** - disabled
6. Save the changes.
7. Close Database Tool (GuiDBEdit Tool).
8. In SmartEndpoint, install policy.

Harmony Endpoint Use Case

Scenario: You see a Threat Emulation or Anti-Bot detection log. What can you do?

Recommendations:

1. From the Forensics, Threat Emulation, or Anti-Bot log, open the Forensics Analysis Report.
2. Open the **Remediation** tab to see the components of the attack and how they were treated.
3. Delete all files that were created by the attack.
4. Open the **Business Impact** tab to see files that might be affected.
5. Open the **Entry Point** tab to see the path of the attack. Update your security policy to prevent similar attacks in the future.

Ransomware Use Case

Scenario: A client computer is attacked by Ransomware. What can you do?

Recommendations:

1. From the Forensics log, open the Forensics Analysis Report.
2. Open the **Remediation** tab to see the components of the attack and how they were treated.
3. If **Automatic restore and remediate** is selected in the **Anti-Ransomware Backup Settings**, restoration and Remediation was triggered and occurs automatically.

   If **Automatic restore and remediate** is NOT selected in the **Anti-Ransomware Backup Settings**, instruct the user to run the Anti-Ransomware Restoration manually from the client computer (see *"Manual Anti-Ransomware Restoration" on page 339*).
4. Analyze the Forensics Analysis Report and update your security policy to prevent similar attacks in the future.

Quarantine Management

When Harmony Endpoint components (Forensics and Anti-Ransomware, Anti-Bot, and Threat Extraction and Threat Emulation), detect malicious files, they can quarantine those files automatically based on policy. All components use the same Remediation service, that:

- Receives the request to quarantine a file.
- Terminates the file's process, if running.
- Encrypts the file and stores it compressed along with metadata in a protected folder.

Two utilities let administrators and end-users manage quarantined files.

Harmony Endpoint Quarantine Manager

The **Harmony Endpoint Quarantine Manager** utility is called **RemediationManagerUI.exe** and it is located in `C:\Program Files (x86)\CheckPoint\Endpoint Security\Remediation` on client computers. It lets end-users:

- See the files in quarantine
- Delete the quarantined files
- Restore files from quarantine.

Harmony Endpoint Quarantine Manager for Administrators

The administrator utility contains the capabilities of the end-user utility plus these additional features:

- **Quarantine** - Send files to quarantine.
- **Delete** - Use the Harmony Endpoint Remediation service to delete a file.
- **Import** - Import a quarantined file from a different computer or location.

You can download the administrator utility from the release homepage.

Using the Quarantine Manager for Administrators

When you open the Harmony Endpoint Quarantine Manager or the Harmony Endpoint Quarantine Manager for Administrators, each quarantined item is shown as a file. The name of the file is the incident ID. To find a file, search for the incident ID found in the Harmony Endpoint logs.

By default, quarantined files stored on the client are in `C:\ProgramData\CheckPoint\Endpoint Security\Remediation\quarantine` on the client computer.

Best practice is to configure **Copy quarantine files to a central location** in the *"File Quarantine Settings" on page 337*. Then you can use the Quarantine Manager for Administrators to import all files related to an incident from one location that you can access.

From the Quarantine Manager for Administrators you can:

- Restore files in a protected location to test them.
- Collect all malicious files related to an attack for research.

To permanently delete an item:

1. Open the Harmony Endpoint Quarantine Manager for Administrators.
2. Select one or more items.
3. Click **Delete**.

To send a file to quarantine from outside of the utility:

1. Open the Harmony Endpoint Quarantine Manager for Administrators.
2. Click **Quarantine**.
3. In the window that opens, browse to select the file to move to quarantine.

To import a suspicious file to the utility:

1. Open the Harmony Endpoint Quarantine Manager for Administrators.
2. Click **Import**.
3. In the window that opens, browse to select the quarantined file to import.

   The file, with its metadata, is imported to the quarantine database from where the utility is run.

Harmony Endpoint Anti-Bot

The Harmony Endpoint Anti-Bot component monitors endpoint computers for bot-related communication and alerts administrators about devices affected by bot activity.

Configure the settings in the **Harmony Endpoint Anti-Bot** rule of in the SmartEndpoint **Policy** tab.

The Need for Anti-Bot

There are two emerging trends in today's threat landscape:

- A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.
- Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.

Both of these trends are driven by bot attacks.

A bot is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.

When a bot infects a computer, it:

- Takes control over the computer and neutralizes its Anti-Virus defenses. Bots are difficult to detect since they hide within your computer and change the way they appear to Anti-Virus software.
- Connects to a Command and Control (C&C) center for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to execute illegal activities without your knowledge. These activities include:
    - Data theft (personal, financial, intellectual property, organizational)
    - Sending SPAM
    - Attacking resources (Denial of Service Attacks)
    - Bandwidth consumption that affects productivity

In many cases, a single bot can create multiple threats. Bots are often used as tools in attacks known as Advanced Persistent Threats (APTs) where cyber criminals pinpoint individuals or organizations for attack. A botnet is a collection of compromised computers.

The Check Point Endpoint Anti-Bot component detects and prevents these bot threats.

The Harmony Endpoint Anti-Bot Solution

The Anti-Bot component:

- Uses the ThreatCloud repository to receive updates and queries it for classification of unidentified IP, URL, and DNS resources.
- Prevents damage by blocking bot communication to C&C sites and makes sure that no sensitive information is stolen or sent out of the organization.

The Endpoint Anti-Bot component uses these procedures to identify bot infected computers:

- Identify the C&C addresses used by criminals to control bots
- These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

Check Point uses the ThreatCloud repository to find bots based on these procedures.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Endpoint Anti-Bot component gets reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified URL/DNS resources that it finds.

Configuring Anti-Bot Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

Activating the Anti-Bot Component

Define the prevention and detection settings for the Anti-Bot component. The automatic options are:

- **Prevents high confidence bots, detects all** - All bots are detected and logged. Anti-Bot only blocks activity when it is almost certain that the activity is malicious (high confidence). This is the default.
- **Anti-bot detection is enabled** -All bots are detected and logged but not blocked.
- **Anti-bot is not active** - Client computers are not monitored for bot activity.

The confidence level is how sure Endpoint Security is that activity is malicious. High confidence means that it is almost certain that the activity is malicious. Medium confidence means that it is very likely that the activity is malicious.

In the **Blade Activation** action, you can manually change the settings for each confidence level.

Select actions for **High Confidence**, **Medium Confidence**, and **Low Confidence** bots:

- **Prevent** - Blocks bots.
- **Detect** - Logs information about bots, but does not block them.
- **Inactive** - Ignores bots (does not prevent or detect them).

Defining Entities that are Trusted by Anti-Bot

By default, the Anti-Bot component inspects all domains.

You can configure trusted entities, which will not be inspected by the Anti-Bot component. These are called Detection Exclusions.

To configure detection exclusions:

1. In the **Properties** of the **Detection Exclusions** Action, select an option from the **Select action** drop-down menu.

   To create a new action profile, click **New**, and in the window that opens enter the name and the description.
2. Click **OK**.
3. Select **Allow detection exclusions for following trusted entities**.
4. Click **Add exclusion**.
5. In the window that opens, select the **Object Type**.

   Click **OK**.

   Enter the name of the new exclusion:

   - **Process** - Name of an executable
   - **URL** - Website URL
   - **Domain** - Full domain name
   - **Protection Name** - Predefined malware signature
   - **IP Range** - Internal or External IP addresses
6. Click **OK**.
7. Click **OK**.

Anti-Bot Protection Mode

By default, the Anti-Bot **Default protection mode** allows connections while it checks for bots in the background. You can choose to block connections until the threat check is complete.

To configure General Settings:

1. In the **Properties** of the **General Settings** Action, select an option from the **Select action** drop-down menu.

   To create a new action profile, click **New**, and in the window that opens enter the name and the description.

2. Click **OK**.
3. Select the default behavior:
   - **Background - connections are allowed until threat check is complete**
   - **Hold - connections are blocked until threat check is complete**
4. **Hours to suppress logs for same bot protection** -To minimize the size of the Anti-Bot logs, actions for the same bot are only logged one time per hour. To change the default log interval , select a number of hours.
5. **Days to remove bot reporting after** -If a bot does not connect to its command and control server after the selected number of days, the client stops reporting that it is infected.
6. Click **OK**.

Harmony Endpoint Threat Extraction, Emulation and Anti-Exploit

Threat Emulation detects zero-day and unknown attacks. Files on the endpoint computer are sent to a sandbox for emulation to detect evasive zero-day attacks.

Threat Extraction proactively protects users from malicious content. It quickly delivers safe files while the original files are inspected for potential threats.

Anti-Exploit protects against application threats that exploit memory vulnerabilities. Anti-Exploit protects widely targeted applications such as Microsoft Office, Adobe PDF Reader, Browsers, and Adobe Flash.

As part of the Threat Extraction and Threat Emulation solution, when the Harmony Endpoint client is installed on a client computer, the Harmony Endpoint Browser Extension is also installed on the Google Chrome browser. The Harmony Endpoint Browser Extension protects against malicious files that come from internet sources.

See all Threat Extraction and Threat Emulation logs in SmartLog under Threat Emulation.

- Logs related to files from the Harmony Endpoint Browser Extension show: **Monitor Type - Browser Extension** and **Browser - Chrome**
- Logs related to files from the computer show: **Monitor Type - File Monitor**

Configure the settings in the **Harmony Endpoint Threat Extraction and Threat Emulation** rule of in the SmartEndpoint **Policy** tab.

Configuring Threat Extraction and Threat Emulation Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

Web Download Protection

Define the settings for the Harmony Endpoint Browser Extension to protect against malicious files that come from internet sources. The Browser Extension is supported on Google Chrome.

The automatic options are:

- **Protect web downloads with Threat Extraction and Emulation** - Send files for emulation. While a file is tested, users receive a copy of it with all suspicious parts removed. If the file is not malicious, users receive the original file when the emulation is finished. Emulation can take up to two minutes.
- **Protect web downloads with Threat Emulation** - Send files for emulation. Users do not receive a copy during the emulation. If the file is not malicious, users receive the original file when the emulation is finished. Emulation can take up to two minutes.
- **Do not use web download protection** - The Harmony Endpoint Browser Extension is not active.

When Threat Extraction is selected, it only applies to file types that can be extracted, such as documents.

When Threat Emulation is selected, it only applies to file types that can be emulated, such as executables and scripts.

You can edit the selections manually to define more settings for Threat Extraction and Threat Emulation for different file types.

To change the setting for categories of file types:

1. In a Harmony Endpoint Threat Extraction and Threat Emulation rule, right-click the **Web Download Protection** Action and select **Edit Shared Action**.
2. Expand the list for the type of file that you choose:
   - **Files that can be extracted and emulated** (such as documents and pictures).
   - **Files that can only be emulated** (such as executables and scripts).
   - **When neither Extraction nor Emulation is supported** (such as videos).
3. Select an option for emulation and access to the original file from the options shown. Different options show for different file types.
   - **Extract and suspend original file until emulation completes** - Send files for emulation. While a file is tested, the user receives a copy of it with all suspicious parts removed.

- **Emulate and suspend original file until emulation completes** - Send files for emulation. Users only receive the files after the emulation finishes and the file was found to be safe.
- **Emulate original file without suspending access** - Send files for emulation. Users can download and access the file while it is tested. The administrator is notified if files are found to be malicious.
- **Allow Download** - No emulation or extraction. The download is allowed.
- **Block Download** - No emulation or extraction. The download is blocked.

4. If files are extracted, select the **Extract Mode**, which is the format of the extracted document that users can see during the emulation.
   - **Extract potentially malicious elements** -The file is sent in its original file type but without malicious elements.
   - **Convert to PDF** - When relevant, files are converted to PDF.
5. Click **OK**.

To change the setting for a specified file type, such as.zip or .pdf:

1. In a Harmony Endpoint Threat Extraction and Threat Emulation rule, right-click the **Web Download Protection** Action and select **Edit Shared Action**.
2. Click **Override default file action per file type**.
3. Select a file type.
4. Click in the **File Action** column to select a different action for that file type.
5. Click in the Extraction Mode column to select a different extraction mode for the file type.
6. Click **OK**.

File System Emulation

Define the default settings for emulation of files on the file system. The automatic options are:

- **Emulate files written to file system** - All files that can be emulated are automatically sent for emulation when they are written to the file system.
- **Do not emulate files written to file system** - Files are not automatically sent for emulation when they are written to the file system.

Monitoring is enabled by default for all options.

Harmony Environment Settings

By default, Harmony Endpoint uses the SandBlast Cloud for Threat Extraction and Threat Emulation.

If you have one or more Harmony Appliances, you can use them as an alternative to SandBlast Cloud.

To configure Harmony Endpoint to work with a Harmony Appliance:

1. In a Harmony Endpoint Threat Extraction and Threat Emulation rule, right-click the **Harmony Environment Settings** Action and select **Edit Shared Action**.
2. Select **Use Harmony Appliance for Threat Extraction and Threat Emulation**.
3. In the Properties of the action, click **Configure Appliances**.
4. In the **Appliances Configuration** window, select an appliance from the list, or click **Add** and enter:
   - **IP address** of the **Harmony Appliance**
   - **Appliance Certificate Name** - Click **Manage** to select a certificate or to import one.
5. To configure a certificate for communication between Harmony Endpoint and the Harmony Appliance, see sk116381.
6. By default the Cloud will be used if the Appliance is not available. If you do not want the SandBlast Cloud to be used as backup, clear the option **If appliance is not available, fallback to Cloud**.
7. Click **OK**.

To define the maximum size of files that are sent for emulation:

1. In a Harmony Endpoint Threat Extraction and Threat Emulation rule, right-click the **Harmony Environment Settings** Action and select **Edit Shared Action**.
2. Change the value for **Upload to emulation files less than X Megabytes**. The default is that file less than 10 MB are sent for emulation.

Exclusions and Inspection Settings

The default behavior is **Inspect all domains and files**. All files in the file system are inspected and sent for emulation when applicable. You can configure exclusions that are not inspected.

Click **Add exclusion** to exclude a file or process from inspection. You can define an exclusion by many different criteria. Criteria include: Domain, folder, and SHA1 hash. Add more information to make the exclusion very specific and less information to make it broad.

Domain exclusions

- To exclude an IP, in the **Element** field, enter IP address followed by subnet mask in the format <X.X.X.X>/ <subnet mask >. For example, to exclude a computer with IP address 192.168.100.30, enter 192.168.100.30/24.
- Domain exclusions must be added without http/s, *, or any other special characters.

  Domain exclusions can be added with or without www.
- Sub-domain exclusions are supported.

  Exclusion of a domain will exclude all its subdomains as well.

For example:

If you enter the domain	It excludes these domains	It does not exclude these domains
www.domain.com	■ https://www.domain.com ■ http://www.domain.com	■ https://domain.com ■ http://domain.com ■ https://sub.domain.com ■ http://sub.domain.com
domain.com	■ https://www.domain.com ■ http://www.domain.com ■ https://domain.com ■ http://domain.com ■ https://sub.domain.com ■ http://sub.domain.com	-
sub.domain.com	■ https://sub.domain.com ■ http://sub.domain.com	https://sub2.domain.com

SHA1 exclusions -

- File Reputation exclusions are set by SHA1.

- Folder path cannot contain environment variables.
- When you exclude a folder, enter the folder as a windows path. For example:

  ```
  C:\Program Files\MyTrustedDirectory\
  ```

Zero Phishing Settings

Define setting for phishing prevention and password reuse prevention.

- **Phishing Prevention** - Checks different characteristics of a website to make sure that a site does not pretend to be a different site and use personal information maliciously.
- **Password Reuse Prevention** - Alerts users not to use their corporate password in non-corporate domains.

Phishing Prevention

- **Phishing Protection** - Select an option:
  - **Prevent Access and Log** (default) - If Harmony Endpoint determines that the site is phishing, users cannot access the site. A log is created for each malicious site.
  - **Off** - Phishing prevention is disabled.
  - **Log Only** - When a user uses a malicious site, a log is created.
  - **Prevent Access Only** - Users cannot access malicious sites. No logs are created.
- **Send log on each scanned site** - Send logs for each site that users visit, if it is malicious or not. By default, it is **not** selected.
- **Allow user to dismiss the phishing alert and continue to access the site** - Users can choose to use a site that was found to be malicious.
- **Allow user to abort phishing scans** - Users can stop the phishing scan before it is completed.

Password Reuse

- **Password Reuse Protection** - Select an option:
  - **Alert User and Log** (default) - If a user enters a corporate passwords in a non-corporate site, the user gets an alert and a log is created.
  - **Off** - Password Reuse Prevention is disabled.
  - **Log Only** - If a user enters a corporate passwords in a non-corporate site, a log is created.
  - **Alert User Only** - If a user enters a corporate passwords in a non-corporate site, the user gets an alert.
- **Protected Domains** - Add domains for which Password Reuse Protection is enforced. Harmony Endpoint keeps a cryptographic secure hash of the passwords used in these domains and compares them to passwords entered outside of the protected domains.

Firewall

Firewall rules allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols. There are two types of Firewall rules:

- **Inbound rules** - Rules that allow or block incoming network traffic to the endpoint computer.
- **Outbound rules** - Rules that allow or block outgoing network traffic from the endpoint computer.

Planning Firewall Policy

When you plan a Firewall Policy, think about the security of your network and convenience for your users. A policy should permit users to work as freely as possible, but also reduce the threat of attack from malicious third parties.

The defined Actions in the Firewall rules make it easy to create the Firewall policy that you choose. Select an Action for Inbound traffic and an Action for Outbound traffic. The required rules are automatically added to the Firewall Inbound and Outbound Rule Bases.

You can add more rules to each Rule Base and edit rules as necessary.

Changes are enforced after the Policy is installed.

Inbound Traffic Rules

Inbound traffic rules define which network traffic can reach endpoint computers (known as **localhost**).

Select an Action:

Action	Description
Allow inbound traffic	Allows all incoming traffic to the endpoint computer,
Allow inbound traffic from trusted zones and connectivity services	Allows all incoming traffic from trusted zones and IP obtaining traffic from the internet. All other traffic is blocked.

The rules required for the selected Action are automatically added to the **Inbound firewall rules** Rule Base.

Right-click an Action to see the **Inbound firewall rules** Rule Base. You can add, delete, and change rules as necessary.

Note - There is no **Destination** column in the Inbound Rule Base because the destination of all traffic is the endpoint computer.

Outbound Traffic Rules

Outbound traffic rules define which outgoing network traffic is allowed from endpoint computers.

Select an Action:

Action	Description
Allow any outbound traffic	Allows all outgoing traffic from the endpoint computer.
Allow outbound traffic to trusted zones and common internet protocols	Allow all traffic to trusted zones and traffic of common internet protocols to the internet.

The rules required for the selected Action are automatically added to the **Outbound firewall rules** Rule Base.

Right-click an Action to see the **Outbound firewall rules** Rule Base. You can add, delete, and change rules as necessary.

Note - There is no **Source** column in an Outbound Rule Base because the source of all traffic is the endpoint computer.

Creating Firewall Rules

Create Firewall rules that relate to inbound traffic in the inbound traffic Rule Base and rules that relate to outbound traffic in the outbound traffic Rule Base.

To create a Firewall rule:

1. In the **Firewall** rule in the **Policy** tab, right-click the inbound or outbound traffic Action and select **Edit Properties**.
2. Click one of the **Add Rule** icons from above the Rule Base.
3. Fill in the columns of the rule. Right-click in a column to select an option.

Column	Description
NO	Rule priority number. Rule priority is important because a client checks Firewall rules based on its sequence in the Rule Base. Rules are enforced from the top to the bottom. The last rule is usually a Cleanup Rule that says to drop traffic that does not match any of the previous rules.
Name	Name of the Firewall Rule.
Source or Destination	■ **Source** - Source location of the network traffic. For an outbound rule, the source is always the local computer. ■ **Destination** - Destination location of network traffic. For an inbound rule, the destination is always the local computer. ■ Source and Destination can be any of the Network Objects defined in the Access Zones policy or the Trusted/Internet Zone.
Service	Network protocol or service used by traffic.
Action	What is done to traffic that matches the rule: **Accept** or **Drop**.
Track	When the rule is enforced: ■ **Log** - Record rule enforcement in the Endpoint Client Log Viewer. ■ **Alert** -Show a message on the endpoint computer and record rule enforcement in the Endpoint Client Log Viewer. ■ **None** - Log and alert messages are not created.

Notes on configuring Tracking:

- If you have a rule that drops or accepts all traffic, do not enable logging.
- To use logs and alerts, you must configure options in the **Client Settings** rules:
  - In the **Log Upload** action, **Enable log upload** must be selected.
  - In the **Users Disabling Network Protection** action, under **Network Protection Alerts**, in the **Firewall** row, select **Allow Alert**.

Firewall Rules and Domain Controllers

Important - When creating Firewall Rules for endpoint clients, create explicit rules that allow all endpoints to connect to all of the domain controllers on the network.

Services and Network Objects

The same Network Objects and Services are used throughout the SmartEndpoint and in SmartConsole. When you create a new object, it is also available in SmartConsole. If you change an object in the SmartEndpoint or SmartConsole, it is changed everywhere that the object is used.

To create a Network Object:

1. In the Inbound or Outbound Firewall Rule Base, open the **Network Objects** tab.
2. Click **New**.
3. Select the type of object from the **New Object Type** list.
4. Click **OK**.
5. In the **Properties** window, enter the required information.
6. Click **OK**.

To create a Service:

1. In the Inbound or Outbound Firewall Rule Base, open the **Services** tab.
2. Click **New**.
3. Select the type of service from the **New Object Type** list.
4. Click **OK**.
5. In the **Properties** window, enter the required information.
6. Optional: If you create a **Group**, In the **Group Properties** window, add **Available Services** to a group.
7. Click **OK**.

Disabling and Deleting Rules

When you delete a rule, it is removed from the Rule Base and not enforced in the policy.

When you disable a rule, the rule is not enforced in the policy. The rule stays in the Rule Base with an X showing that it is disabled. Select **Disable rule** again to make the rule active.

To delete or disable a rule:

1. Right-click in the **NO** column of a rule
2. Select **Delete Rule** or **Disable Rule**.
3. Install policy.

The rule is not physically deleted or disabled until you install the policy.

Wireless Connection Settings

These actions define if users can connect to wireless networks while on your organization's LAN. This protects your network from threats that can come from wireless networks.

Action	Description
Allow connecting wireless to LAN	Users can connect to wireless networks while connected to the LAN
Do not allow connecting wireless to LAN	Users cannot connect to wireless networks while connected to the LAN.

Hotspot Settings

These actions define if users can connect to your network from hotspots in public places, such as hotels or airports.

Action	Description
Allow hotspot registration	Bypass the Firewall to let users connect to your network from a hotspot.
Do not allow hotspot registration	Do not let users connect to your network from a hotspot.

IPv6 Traffic

You can select one of these actions to allow or block IPv6 traffic to endpoint computers.

- Allow IPv6 network traffic
- Block IPv6 network traffic

Choosing a Firewall Policy to Enforce

By default, the Firewall policy enforced is the Endpoint Security Firewall Policy Rules.

If your environment had Endpoint Security VPN and then moved to the complete Endpoint Security solution, you might want to continue to use the Desktop Policy from the legacy SmartDashboard that you open from SmartConsole. To learn how to configure a Desktop Policy, see *Managing Desktop Firewalls* in the *Remote Access clients for Windows Administration Guide for your client release*.

Select which Firewall policy to enforce:

Action	Description
Enforce Endpoint Firewall policy	Use the Endpoint Security Firewall Policy Rules
Enforce Desktop Policy from SmartConsole	Use the Desktop Policy from SmartConsole

To activate the Desktop Policy from SmartConsole:

1. In the SmartEndpoint **Policy** tab, go the **Firewall** section of the policy.
2. In the **Actions** column, select **Enforce Desktop Policy from SmartConsole**.
3. Install Policy.
4. Restart all computers included in the rule.

Compliance

The Compliance component of Endpoint Security makes sure that endpoint computers comply with security rules that you define for your organization. Computers that do not comply show as non-compliant and you can apply restrictive policies to them.

The Compliance component makes sure that:

- All assigned components are installed and running on the endpoint computer.
- Anti-Malware is running and that the engine and signature databases are up to date.
- Required operating system service packs and Windows Server updates are installed on the endpoint computer.
- Only authorized programs are installed and running on the endpoint computer.
- Required registry keys and values are present.

  Note - Registry and File Version checks are not relevant for macOS

If an object (for example an OU or user) in the organizational tree violates its assigned policy, its compliance state changes, and this affects the behavior of the endpoint computer:

- The compliant state is changed to non-compliant.
- The event is logged, and you can monitor the status of the computer and its users.
- Users receive warnings or messages that explain the problem and give a solution.
- Policy rules for **restricted** computers apply. See *"Connected, Disconnected and Restricted Rules" on page 170*.

Planning for Compliance Rules

Before you define and assign compliance rules, do these planning steps:

1. Identify the applications, files, registry keys, and process names that are required or not permitted on endpoint computers.
2. Collect all information and Remediation files necessary for user compliance. Use this information when you create Remediation objects to use in compliance rules.

   Compliance rules can prevent users from accessing required network resources when they are not compliant. Think about how to make it easy for users to become compliant.
3. Make sure that the Firewall rules gives access to Remediation resources. For example, sites from which service packs or Anti-virus updates can be downloaded.

   Note - In Windows 7, make sure the **Interactive Service Detection** service is running. This is necessary for Remediation files (running with system credentials) that must interact with the user.
4. Define rule alerts and login policies to enforce the rules after deployment.

Configuring Compliance Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

Ensuring Alignment with the Deployed Profile

This action the Compliance policy makes sure that all installed components are running and defines what happens if they are not running. The action options are:

Action	Description
Inform if assigned Software Blades are not running	Send a warning message if one or more Endpoint Security components are not running.
Restrict if assigned Software Blade are not running	Restrict network access if one or more Endpoint Security components are not running.
Monitor if assigned Software Blades are not running	Create log entries if one or more Endpoint Security components are not running. No messages are sent.
Do not check if assigned Software Blades are not running	No check is made whether Endpoint Security components are running.

VPN Client Verification

The VPN Client Verification action selects the procedure used to enforce the **Upon verification failure** option that is defined in SmartConsole, in **Menu** > **Global Properties** > **Remote Access** > **Secure Client Verification (SCV)**. The procedures are:

- **VPN Client verification process will use Endpoint Security Compliance** - Uses the Endpoint Security policy to control access to organizational resources.
- **VPN Client verification process will use VPN SCV Compliance** - Uses SCV (Security Configuration verification) settings from the Security Gateway to control access to organization resources. SCV checks, which are defined in the **Local.scv** policy, always run on the client. This option is described in the "*Secure Configuration Verification (SCV)*" section of the *Remote Access VPN Client for Windows Administration Guide*.

  Note - Endpoint Security clients on Mac always get their compliance status from Endpoint Security Compliance, even if **VPN Client verification process will use VPN SCV Compliance** is selected.

Compliance Action Rules

Many of the Compliance Policy actions contain **Action Rules** that include these components:

- **Check Objects (Checks)** - Check objects define the actual file, process, value, or condition that the Compliance component looks for.
- One or more **Remediation** objects - A Remediation object runs a specified application or script to make the endpoint computer compliant. It can also send alert messages to users.
- One of these **Action** options - What happens when a computer violates the rule:

Action	Definition
Observe	Log endpoint activity without further action. Users do not know that they are non-compliant. Non-compliant endpoints show in the **Observe** state in the **Reporting** tab.
Warn	Alerts the user about non-compliance and automatically does the specified Remediation steps. Send a log entry to the administrator.
Restrict	Alerts the user about non-compliance and automatically does the specified Remediation steps. Send a log entry to the administrator. Changes applicable polices to the restricted state after a pre-defined number of heartbeats (default =5). Before this happens, the user is in the *about to be restricted* state. On the monitoring tab, the user is shown as *pre-restricted.*

The Compliance component runs the rules. If it finds violations, it runs the steps for Remediation and does the Action in the rule.

Some Action Rules are included by default. You can add more rules for your environment.

Basic Workflow for defining additional compliance rules:

1. In the **Policy** tab, right-click an action in the **Actions** column and select **Edit Properties**.
2. Click **Create Rule** to create new **Action Rules** as necessary:
   a. In the **Name** field, enter the Action rule name.
   b. Click **Check** to add Check objects to add to the Action *"Compliance Check Objects" on the next page*.
   c. Select an **Action** from the list.

d. Click the **Remediation** tab to add Remediation objects to the *"Compliance Remediation Objects" on page 384*. If the selected **Action** is **Observe**, the rule does not require a Remediation object.

e. Optional: In the **Comment** field, enter a comment for the action rule.

Do these steps again to create additional Action rules as necessary.

Compliance Check Objects

Each Compliance Action Rule contains a **Check** object that defines the actual file, process, value or condition that the Compliance component looks for.

To create a new or change an existing Check object:

1. In the **Edit Properties** window of a Compliance Action, click **View Objects List**.
2. Click **New** to create a new Check object, or **Edit** to change an existing one.
3. For **Required applications and files** only: When you create a new Check object, select an **Object Type**:
   - **Required Entity Check** - Add one specified file Check object.
   - **Required Entity Group** - Add a group of Check objects that must all be on the computer.
4. In the **Compliance Check Properties** window, fill in these fields.

Option	Description
Name	Unique name for this Check Object.
Comment	Optional: Free text description
Operating System	Select the operating system that this Check object is enforced on.
Check Registry	Select one of these options to enable the registry check or clear to disable it: **Registry key and value exist** - Find the registry key and value. If the registry key exists, the endpoint computer is compliant for the required file. **Registry key and value do not exist** - Make sure the registry key and value do not exist. If the key does not exist, the endpoint computer is compliant for an application that is prohibited.

Option	Description
Registry Key	Enter the registry key.
Registry Value	Enter the registry value to match.
Check File	Select one of these options to check if an application is running or if a file exists: **File is running at all times** - For example, make sure that Endpoint Security client is always running. **File exists** - For example, make sure that the user browsing history is always kept. **File is not running** - For example, make sure that DivX is not used. **File does not exist** - For example, make sure that a faulty DLL file is removed.
File Name	Enter the name of the file or executable to look for. To see if this file is running or not, you must enter the full name of the executable, including the extension (either .exe or .bat).
File Path	Enter the path without the file name. Select the **Use environment Variables of logged in user** option to include paths defined in the system and user variables. Do not add the "\" character at the end of the path.
Check File Properties	Additional options to check for an existing or non-existing file.
Match File Version	Make sure that a specific version or range of versions of the file or application complies with the file check.
Match MD5 Checksum	Find the file by the MD5 Checksum. Click **Calculate** to compare the checksum on the endpoint with the checksum on the server.
File is not older than	Select this option and enter the maximum age, in days, of the target file. If the age is greater than the maximum age, the computer is considered to be compliant. This parameter can help detect recently installed, malicious files that are disguised as legitimate files.

5. Optional: You can select or define a **Remediation** action for this Check object.

   The Remediation action applies only to this Check object and overrides the Remediation action specified in the rule. To define a Check object Remediation action, select a Remediation action from the list or click **Remediation** tab > **New** to define a new one.

Compliance Remediation Objects

Each Compliance Action Rule contains one or more **Remediation** objects. A Remediation object runs a specified application or script to make the endpoint computer compliant. It can also send alert messages to users.

After a **Remediation object** is created, you can use the same object in many Action rules.

To create a new or change an existing Remediation object:

1. In the **Edit Properties** window of a Compliance Action, click **View Objects List**.
2. Select the **Remediations** tab and click **New**.
3. In the **Remediation Properties** window, fill in these fields:

Option	Description
Operations	
Run Custom File	Run the specified program or script when an endpoint computer is not compliant.
Download Path	■ Enter the temporary directory on the local computer to download the program or script to. This path must be a full path that includes the actual file and extension (*.bat or *.exe). ■ This parameter is required. ■ The endpoint client first tries to access the file from the specified path. If the client fails, it downloads the file from the URL to the temporary directory and runs it from there. ■ To run multiple files, use one of the popular compression programs such as *WinRAR* to produce a self-extracting executable that contains a number of .exe or .bat files.
URL	■ Enter the URL of an HTTP or file share server where the file is located. ■ Enter the full path that includes the actual file with one of the supported extensions (*.bat or *.exe). ■ This field can be left empty. ■ Make sure the file share is not protected by a username or password.

Option	Description
Parameters	If the executable specified in the URL runs an installation process, make sure that the executable holds a parameter that specifies the directory where the program should be installed. If the executable does not hold such a parameter, enter one here.
MD5 Checksum	Click **Calculate** to generate a MD5 Checksum, a compact digital fingerprint for the installed application or the Remediation files.
Run as System	Apply system rights for running the executable file. Not all processes can run with user rights. System rights may be required to repair registry problems and uninstall certain programs.
Run as User	Apply user rights and local environment variables for running the executable file.
Messages	
Automatically execute operation without user notification	Run the executable file without displaying a message on the endpoint computer.
Execute operation only after user notification	Run the executable file only after a user message opens and the user approves the Remediation action. This occurs when **Warn** or **Restrict** is the selected action on a compliance check.
Use same message for both Non-Compliant and Restricted messages	Select that the same text be used for both messages. A Non-Compliant message tells the user that the computer is not complaint and shows details of how to become compliant. A Restricted message tells the user that the computer is not compliant, shows details of how to achieve compliance, and restricts computer use until compliance is achieved.
Message Box	Displays selected non-compliant and restricted messages. The message box is available only by selecting the Execute only after user notification setting. Click **Add**, **Remove**, or **Edit** to add a message, and remove or revise a selected message. **Note**: User cannot prevent the Remediation application or file from running.

Service Packs for Compliance

The **Service Packs Compliance** Action makes sure that computers have the most recent operating system service packs and updates installed. The default settings show in the **Latest Service Packs Installed** Action Rules.

See *"Compliance Action Rules" on page 381* for more information.

Required Applications and Files

Required Application and File Compliance Settings look for the presence of specified files, registry values, and processes that must be running or present on endpoint computers. The default settings show in the **Required Application** Action Rules.

For **Required Application** action rules, multiple check objects in the rule are mutually exclusive. If one or more check object is not compliant, the defined action and Remediation is triggered.

See *"Compliance Action Rules" on page 381* for more information.

Prohibited Applications and Files

The **Prohibited Applications and Files** Action makes sure that files, registry keys, and processes that must not be on endpoint computers are not present or running. The default settings show in the **Prohibited Application** Action Rules.

For Prohibited **Application** action rules, all check objects must be non-compliant to trigger the action and Remediation. If only one check object is compliant, the action and Remediation are not triggered.

See *"Compliance Action Rules" on page 381* for more information.

Anti-Malware for Compliance

The Anti-Malware check makes sure that computers have an anti-malware program installed and updated. The default settings show in the **Anti-Malware Compliance** Action Rules.

See *"Compliance Action Rules" on page 381* for more information.

Ensuring that Windows Server Updates Are Installed

Windows Server Update Services (WSUS) allows administrators to deploy the latest Microsoft product updates.The WSUS compliance check ensures that Windows update are installed on the Endpoint Security client computer. You can restrict network access of the client computer if Windows updates have not been installed within a specified number of days. Alternatively, you can warn the user by means of a pop-up message without restricting access, or log the non-compliance event without restricting or informing the user

To configure the WSUS compliance check:

1. In the **Policy** tab **Compliance** rule, right-click the **Windows Server Update Services** action
2. Select one of the following preset actions. An action happens if Windows updates have not been installed on the Endpoint Security client computer for a specified number of days (90 days by default):

Preset Action	Meaning
Restrict if Windows Server Updates are not installed	Restrict the network access of the user.
Observe Windows Server Update Services	Create a log, and show a warning message to the user.
Monitor Windows Server Update Services	Create a log. The user is not notified.
Do not check Windows Server Update Services	No compliance check. This is the default.

3. **Optional**: The compliance check makes sure that the Windows updates have been installed within a specified number of days (90 by default). To change the number of days,
    a. Right-click the **Windows Server Update Services** action.
    b. Select **Edit Shared Action**.
    c. Change the number of days in **Windows updates must be installed within**.

Monitoring Compliance States

Monitor the compliance state of computers in your environment from:

- The **Logs** tab of the SmartConsole Logs & Monitor view
- The Security Overview
- **Reporting** > **Compliance**

These compliance states are used in the Security Overview and Compliance reports:

- **Compliant** - The computer meets all compliance requirements.
- **About to be restricted** - The computer is not compliant and will be restricted if steps are not done to make it compliant. See *"Configuring the "About to be Restricted" State" on the next page*
- **Observe** - One or more of the compliance rules that is set as **Observe** is not met. Users do not know about this status and have no restrictions.
- **Restricted** - The computer is not compliant and has restricted access to network resources.
- **Warn** - The computer is not compliant but the user can continue to access network resources. Do the steps necessary to make the computer compliant.

The Heartbeat Interval

Endpoint clients send "heartbeat" messages to the Endpoint Security Management Server to check the connectivity status and report updates. The time between heartbeat messages is known as the *heartbeat interval.*

Note - The default heartbeat interval is 60 seconds. A shorter heartbeat interval can cause additional load on the management. A longer heartbeat interval may lead to less up-to-date logs and reports

The endpoint computer Compliance state is updated at each heartbeat. The heartbeat interval also controls the time that an endpoint client is in the **About to be restricted** state before it is restricted.

It is possible to create restricted policies that will automatically be enforced once the endpoint client enters a restricted state

To configure the heartbeat interval and out-of-compliance settings:

1. Click **Manage > Endpoint Connection Settings**.

   The **Connection Settings Properties** window opens.

2. In the **Connection Settings** section, set the **Interval between client heartbeats**.

3. In the **Out-Of-Compliance** section, configure when a client is restricted. Configure the number of heartbeats in **Client will restrict non compliant endpoint after**. The default is 5 heartbeats.
4. Click **OK**.

Configuring the "About to be Restricted" State

The **About to be restricted** state sends users **one last warning** and gives an opportunity to immediately correct compliance issues before an endpoint computer is restricted. You can configure the period of time that a user has to correct the issues after the warning message shows.

You define this period of time in heartbeats.

To configure the time period that users have before an endpoint computer is restricted:

1. Click **Manage > Endpoint Connection Settings**.

   The **Connection Settings Properties** window opens.
2. In the **Out of Compliance** section, enter the number of heartbeats.
3. Click **OK**.

When you configure this time period, we recommend that you give users sufficient opportunity to:

- Save their data.
- Correct the compliance issues.
- Make sure that the endpoint computer is compliant.

The formula for converting the specified time period to minutes is:
`<number of heartbeats > * <heartbeat interval (in seconds)> * 60.`

Application Control

The Application Control component of Endpoint Security restricts network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes. The administrator can also configure that an application will be terminated when it tries to access the network, or as soon as the application starts. .

You can also enable the Reputation Service (previously called the Program Advisor).The Reputation Service recommends whether to approve or not approve an application, and the Endpoint Security client uses that recommendation , together with the permission setting for that application in the Application Control policy to decide whether to Allow or block the application.

This is the workflow for configuring Application Control:

1. Set up a Windows computer with the typical applications used on protected endpoint computers in your organization. This is your reference computer. If you have several different standard images, set up a reference computer for each.
2. Generate the list of applications on the computer by running the `Appscan` tool. This generates an XML file that contains the details of all the applications on the computer.
3. Import the `Appscan` XML file to the Endpoint Security Management Server using SmartEndpoint.
4. Configure how the Application Control policy handles applications that are imported from the `Appscan` XML file. By default, the applications are allowed.
5. **Optional**: In the Application Control Policy, review the permission that was automatically configured for each application and application version. You can configure which applications are allowed, blocked, or terminated.
6. **Optional**: Enable the Reputation Service. This is an online service that recommends whether to approve or not approve an application. The Endpoint Security client uses the recommendation of the Reputation Service, together with the permission setting for that application in the Application Control policy to decide whether to Allow or Block the application.
7. Install the Application Control policy.

Creating the List of Applications on the Reference Computer

You need to generate a list of the application on your reference computer. This is a Windows computer with a tightly-controlled disk image that contains the typical applications used on protected endpoint computers in your organization. If you have several different standard images, set up a reference computer for each.

Important - The reference computer must be free of malware.

To generate the list of applications, run, the `Appscan` command on the reference computer. This generates an XML file that contains the details of all the applications and operating system files on the computer. In the XML file, each application, and each application version, is uniquely identified by a checksum. A checksum is a unique identifier for programs that cannot be forged. This prevents malicious programs from masquerading as other, innocuous programs.

To run Appscan from the command line:

1. Download the `appscan` tool from sk108536, to the root directory (typically `c:\`) of the baseline reference source computer.
2. From the command prompt of the target computer, go to the root directory or to a specific directory to scan (for example, `\program files`).
3. Run `appscan` with the applicable parameters.

When the scan is complete, an output file is created in the specified directory. The default file name is `scanfile.xml`

Appscan Command Syntax

Description

Scans the host computer and creates an XML file that contains a list of executable programs and their checksums. This XML file is used by the Check Point Reputation Service to create recommended rules to block or allow common applications. The administrator imports the XML file to theEndpoint Security Management Server using SmartEndpoint.

Syntax

```
Appscan [/o <filename> /s <target directory> /x <extension strung
/e /a /p /verbose /warnings /?
```

Parameters

Parameter	Description
`/o`	Sends output to the specified file name. If no file name is specified, `Appscan` uses the default file name (`scanfile.xml)` in the current folder.
`file name`	Output file name and path.
`/s <target directory>`	Specifies the directory, including all subdirectories, to scan. ■ You must enclose the directory/path string in double quotes. ■ If no directory is specified, the scan runs in the current directory only.
`/x <extension string>`	Specifies the file extension(s) to include in the scan. ■ The extension string can include many extensions, each separated by a semi-colon. ■ You must put a period before each file extension. ■ You must enclose full extension string in double quotes. ■ You must specify a target directory using the /s switch. ■ If you do not use the `/x` parameter only `.exe` executable files are included in the scan
`/e`	Include all executable files in the specified directory regardless of the extension. Do not use `/e` together with `/x`.
`/a`	Includes additional file properties for each executable.
`/p`	Shows progress messages during the scan.
`/verbose`	Shows progress and error messages during the scan.
`/warnings`	Shows warning messages during the scan.

`/?`
or
`/help`
	Shows the command syntax and help text.

Examples

- `appscan /o scan1.xml`

  This scan, by default, includes .exe files in the current directory and is saved as `scan1.xml`.

- `appscan /o scan2.xml /x ".exe;.dll" /s "C:\"`

  This scan includes all .exe and .dll files on drive C and is saved as `scan2.xml`.

- `appscan /o scan3.xml /x ".dll" /s c:\program files`

  This scan included all .dll files in `c:\program files` and all its subdirectories. It is saved as `scan3.xml`.

- `appscan /s "C:\program files" /e`

  This scan includes all executable files in `c:\program files` and all its subdirectories. It is saved as the default file name `scanfile.xml`.

Importing the Appscan XML File to the Endpoint Security Management Server

After you generate the Appscan XML file, import it to the Endpoint Security Management Server.

Before Importing the Appscan XML file

Remove all special characters, such as trademarks or copyright symbols, from the Appscan XML file.

To import an Appscan XML file:

1. In the **Policy** tab > **Application Control** rule, in the **Actions** column, right-click one of upper four actions. For example **Allowed applications**.
2. Select **Import Programs**.
3. In the **Import Programs** window, click **Browse**, and select the Appscan XML file.
4. Click **Import**.

Configuring If Imported Applications Are Allowed or Blocked by Default

Configure applications that were imported from the Appscan XML file to be Allowed or Blocked by default.

To configure if imported applications are allowed or blocked:

In the **Policy** tab > **Application Control** rule, select one of the following:

- **Allow Unidentified Applications** - This is the default action. In the list of applications, the permission that shows is **Unidentified (Allow)**.
- **Block Unidentified Applications** - In the list of applications, the permission that shows is **Unidentified (Block)**.

An unidentified application is an application that has been imported using the `Appscan` utility, that the administrator has not explicitly classified as Allowed or Blocked.

Configuring Application Permissions in the Application Control Policy

In the Application Control Policy, review the permissions for applications for each application and application version.

For applications and application versions that you are know are secure, change the permission setting to **Allow** .

If you know the applications or application versions are not secure, change the permission setting to **Block**.

You can also configure that blocked applications will be *terminated* when they are started, or when they try to establish a network connection.

To review the policy settings for applications and application versions:

1. In the **Policy** tab > **Application Control** rule, right-click the **Allow Applications** Action and select **Manage All Applications**
2. The **Product Rules** section shows the details for each product, and the **Permission** for each:

Permission	Explanation
Unidentified (Allow)	The application is allowed because the setting for applications that are imported from the Appscan XML.is **Allow unidentified applications**, and the application has not been configured by the administrator as **Allow** or **Block**.
Unidentified (Block)	The application is allowed because the setting for applications that are imported from the Appscan XML.is **Block unidentified applications**, and the application has not been configured by the administrator as **Allow** or **Block**.
Allow	The application has been explicitly configured by the administrator to be allowed. This setting overrides the classification of the Reputation Service of an application.
Block	The application has been explicitly configured by the administrator to be blocked. This setting overrides the classification of the Reputation Service of an application.
Terminate	The application is terminated when it tries to access the network or immediately when it runs.

The **Versions for Application** section shows the details for each version of the application, including a unique hash value that identifies the signer of the application version.You can block or allow specific versions of the same program. Each version has a unique **Version** number, **Hash**, and **Created On** date.

To configure the allowed applications:

1. In the **Policy** tab > **Application Control** rule, right-click the **Allow Applications** Action and select **Manage All Applications**.
2. For applications and application versions that you know are secure, right-click the application and change the permission setting to **Allow** .
3. Click **Close**.

Users can only use applications that are included in the **Allowed Applications List**. Those are applications with the status **Unidentified (Allow)** and **Allow**.

To configure the blocked applications:

1. In the **Policy** tab > **Application Control** rule, right-click the **Blocked Applications** Action and select **Manage All Applications**.
2. For applications and application versions that you are know are not secure, right click the application and change the permission setting to **Block**.
3. Click **Close**.

Users cannot use applications that are included in the **Blocked Applications List**. Those are applications with the status **Unidentified (Block)**, **Block** and **Terminated**.

To configure terminated applications:

1. Configure the Endpoint Security clients and the Compliance policy to make it possible to terminate applications on the clients. See sk141692.
2. In the **Policy** tab > **Application Control** rule, right-click the **Blocked Applications** Action and select **Manage All Applications** .
3. To terminate an application when the application tries to access the network, right click the application and select **Move product to Terminate**. Applications that you select but do not communicate with the network (for example, Windows Notepad and Calculator) are not terminated.
4. Click **Close**.
5. **Optional**: To make sure that all terminated applications terminate immediately when they run:

a. Right-click the **Terminated Applications** Action and select **Manage Terminated Applications List**.

b. Select **Terminate on execution**.

Using the Reputation Service to Allow or Block Applications

The Check Point Reputation Service is an online service that gathers information about applications and classifies them as approved or not approved. The classifications are based on the recommendations of Check Point security experts and the hash value of the signed certificate of the application.

The Endpoint Security client uses the recommendation of the Reputation Service for the application, together with the permission setting for the application in the Application Control policy, to decide whether to allow or block the application.

For example, if an application is configured in the Application Control Policy as **Unidentified (Allow)**, and the Reputation Service recommendation for the application is Not Approved, the application is blocked. However, if the administrator explicitly configures the Application Control policy to Allow or Block the application, the policy setting overrides the recommendation of the Reputation Service.

The Endpoint Security client allows or blocks applications according to the following logic:

Reputation Service recommendation for the application	Application Control Policy setting for the application	Decision by the Endpoint Security Client
Approved	■ (Unidentified) Allow ■ (Unidentified) Block ■ Allow	Allow
Approved	■ Block	Block
Not Approved	■ (Unidentified) Allow ■ (Unidentified) Block ■ Block	Block
Not Approved	■ Allow	Allow

Pre-Requisites for Using the Reputation Service

- The Endpoint Security Management Server must have Internet access (on ports 80 and 443) to connect to the Check Point Reputation Service Server. Make sure that this traffic is allowed.
- We recommend that you add the Reputation Service Server to your Trusted Zone. See *"Changing the Access Zones Policy" on page 419*.

Using the Reputation Service with a Proxy

If your environment includes a proxy server for Internet access, do the configuration steps below to let the Endpoint Security Management Server connect to the Check Point Reputation Service Server through the proxy server. Note that all configuration entries are case-sensitive.

If your organization uses a proxy server for HTTP and HTTPS traffic, you must configure the Endpoint Security Management Server to work with the proxy server.

To configure use of a proxy server:

1. From the Endpoint Security Management Server command line, run: `cpstop`.
2. Go to `$UEPMDIR/engine/conf` and open the `local.properties` file in a text editor.
3. Add a line for these properties:
   - The proxy server IP address:

     `http.proxy.host=<IP address>`
   - The proxy server listening port (typically 8080):

     `http.proxy.port=<port>`
   - If authentication is enabled on the proxy server, add these lines:

     Do not add these lines if authentication is not required.

     `http.proxy.user=<username>`

     `http.proxy.password=<password>`

   Make sure that you delete (or do not insert) the '#' character at the beginning of these lines. If you do not do this, all applications are blocked when trying to access the Internet.
4. Save `$UEPMDIR/engine/conf/local.properties` and then close the text editor.
5. Run: `cpstart`.

Enabling the Reputation Service

In the **Policy** tab > **Application Control** rule, select the action: **Enable Reputation Service**.

Disabling or Enabling Windows Subsystem for Linux (WSL)

Windows Subsystem for Linux (WSL) is the scripting language in Windows 10 and higher. It makes it possible to run Linux binary executables under Windows. WSL has the potential for compromising security.

To enable or disable Windows Subsystem for Linux (WSL) on Endpoint Security client computers:

1. In the SmartEndpoint **Policy** tab, open the **Application Control** rule.
2. Click **Disable WSL Traffic** or **Enable WSL Traffic**.

Preventing the Leakage of Sensitive Information Through Git (Developer Protection)

Developer Protection prevents developers leaking sensitive information such as RSA keys, passwords, and access tokens though the Git version control system. It also warns the developer when vulnerable external dependencies are used in AWS Lambda.

Developer Protection intercepts `git commit` commands issued by the developer, and scans all modified files in a Git repository. It prevents the uploading of private information in plain text from Endpoint Security client computers to public locations.

Developer protection is supported on Endpoint Security Client release E82.50 and higher.

To configure Developer protection:

1. In the SmartEndpoint **Policy** tab, open the **Application Control** rule.
2. Click the **Developer Protection** action and choose an option:

Option	Explanation
Disabled	Developer Protection is disabled. This is the default.
Detect mode	■ Information leakage is detected and a log message is generated, but the Commit is allowed. ■ The administrator can examine the audit log *Detect* messages of the Application Control component. ■ The developer sees a notification on the client computer.
Prevent mode	■ Information leakage is detected, a log message is generated, and the Commit is blocked. ■ The administrator can examine the audit log *Prevent* messages of the Application Control component. ■ The developer sees a warning notification on the client computer.The developer can decide to override the notification and allow the traffic (with or without giving a justification). ■ The notification message suggests how to fix the problem. For example, by adding a file to `.gitignore`, or updating the version in `package.json`

3. Install the Application Control Policy. See *"Installing the Application Control Policy " on page 407*.

Client-Side Warning Notifications

- **Detect Mode** - The user at the Endpoint Security client computer sees a warning message. The user clicks **OK** and continues with the Commit.
- **Prevent Mode** - The user at the Endpoint Security client computer sees a warning message. The user clicks **Cancel** to prevents a Commit. **More Options** allows the user to give a justification and continue with the Commit.

Installing the Application Control Policy

Changes to the Application Control policy are saved immediately. Refreshing the data does not revert the changes.

To install the Application Control policy:

1. In the **Policy** tab, go to the Policy Toolbar.
2. Click Install 

Client Settings

In a large organization, creating a common policy for multiple clients eases deployment and reduces maintenance tasks.

Configuring Client Settings Policy Rules

The Client Settings Actions in the rules set:

- General user interface settings
- If users can postpone installations and for how long.
- The client uninstall password
- When log files are uploaded to the server
- Specified Network Protection settings

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

Client User Interface Settings

You can choose the default client user interface settings or edit them to customize the Endpoint Security client interface on user computers.

You can change these settings:

- **Display client icon** - When selected, the client icon shows in the windows notification area when the Endpoint Security client is installed.
- **Show UserCheck messages** - Define how many UserCheck messages a user may see. These notifications are configured in the *"UserCheck Actions" on page 305* for Media Encryption & Port Protection, and in other places.

  The notification options are:

  - **Show only critical notifications**
  - **Show notifications when protections affect user experience (recommended)**
  - **Show all notifications**
- **Graphics that show in the Pre-boot and OneCheck Logon** - For each of these graphics, you can **Select** to upload a new image or **Revert to Default** image:

Item	Description	Size of Image
Pre-boot Background Image Legacy Resolution (800 x 600)	Legacy resolution image for the Pre-boot screen behind the smaller logon window	800 x 600 pixels
Pre-boot Background Image High Resolution	High resolution image for the Pre-boot screen behind the smaller logon window. For UEFI clients.	1920x1080 pixels
Pre-boot Banner Image	The banner image on the smaller logon window	447 x 98 pixels
OneCheck Logon Background Image	Image in the background of the Windows logon window if OneCheck Logon is enabled	256 KB or smaller
Client Notification (UserCheck) Icon	Icon in the top-right of a Client Notification (UserCheck)	135x46 pixels

Log Upload

The components upload logs to the Endpoint Policy Server

The default log upload Action is **Allow log upload to Endpoint Policy Servers**.

You can change these settings:

Item	Description
Enable Log Upload	Select to enable log upload. Clear to disable log upload. (Default= Selected)
Log upload interval	Frequency in minutes between logged event uploads. The clients upload logs only if the number of logs is more than the **Minimum number of events before attempting an upload**. (Default = 20 minutes)
Minimum number of events before attempting an upload	Upload logged events to the server only after the specified number of events. (Default = 10)
Maximum number of events to upload	Maximum number of logged events to upload to the server. (Default = 100)
Maximum age of event before upload	**Optional**: Upload only logged events that are older than the specified number of days. (Default=5 days)
Discard event if older than	**Optional**: Do not upload logged events if they are older than the specified number of days. (Default = 90 days)
Maximum interval between status updates of Push Operations	*Log Upload* are operations that the Endpoint Security Management Server pushes directly to client computers with no policy installation required. (Default = 5 minutes)

Installation and Upgrade Settings

The default installation and upgrade setting is that users can postpone the Endpoint Security Client installation or upgrade.

You can change these settings:

Item	Description
Default reminder interval	Set the time, in minutes, after which users are reminded to install the client.
Force Installation and automatically restart after	Set the time, in hours, after which the installation starts automatically.
Client Uninstall Password	Set a password that the end user must enter before uninstalling the client. It can contain only English alphabets (upper or lower case), digits and these special characters: `~ = + - _ ( ) ' $ @ , .` The Endpoint Security client has an uninstall password to ensure that only authorized personnel can uninstall the client. The default uninstall password is "`secret`". **Best Practice** - For security reasons, we strongly recommend that you change the default uninstall password.
Legacy Client Uninstall Password	Set a password that the end user must enter before uninstalling a legacy client. The Endpoint Security client has an uninstall password to ensure that only authorized personnel can uninstall the client. The default uninstall password is "`secret`". **Best Practice** - For security reasons, we strongly recommend that you change the default uninstall password.
Uninstall client using dedicated tokens in addition to password	Require a dynamic token challenge-response session, supplied by the administrator, to uninstall the client. This is in addition to the **Client Uninstall Password**. Click **Assign Token** to add a token to the list.

Users Disabling Network Protection

You can let users disable network protection on their computers.

Important - If users disable network protection, their computers will be less secure and vulnerable to threats.
If the policy does not allow users to disable network protection, administrators can assign permissive policies to temporarily disable network protection for specified users.

Network Protection includes these components:

- Firewall
- Application Control

Item	Description
Allow users to disable network protection on their computers	A **Disable Network Protection** option shows in the right-click menu of the client icon from the notification area.
Do not allow users to disable network protection on their computers	Only an administrator can disable a user's network protection.

To configure the Network Protection Alerts :

1. In the **Policy** tab, **Client Settings** rule, double-click the **Network Protection** Action.
2. Click **Edit Properties**.
3. In the **Network Protection** section, select or clear these options for each component:
   - **Allow Log** - To generate logs for events.
   - **Allow Alert** - To generate alerts for events. You must also select this to use **Alert** in the **Track** column of Firewall rules.

Sharing Data with Check Point

Clients can share information about detected infections and bots with Check Point. The information goes to ThreatCloud, a Check Point database of security intelligence that is dynamically updated using a worldwide network of threat sensors. ThreatCloud helps to keep Check Point protection up to date with real-time information.

Note - Check Point does not share any private information with third parties.

To configure data ThreatCloud sharing:

1. In the **Properties** of the **ThreatCloud Sharing** Action, select an option from the **Select action** drop-down menu.

   To create a new action profile, click **New**, and in the window that opens enter the name and the description.

2. Click **OK**.
3. Select or clear:
   - **Enable sharing data with Check Point** (default)
   - **Disable sharing data with Check Point**
4. Click **OK**.

Smart App Control

Smart App Control is a Windows 11 native feature that blocks malicious, untrusted, or potentially unwanted apps from running on your device. For more information, see Smart App Control.

The Smart App Control feature is compatible only with the Harmony Endpoint Security Client E87.50 and higher, with these limitations:

- Only these installations are supported:
  - The **Export Package** must have a custom signature certificate and the packages are signed with these certificates. To create a custom signature, see *"Configuring Software Signatures for Packages for Export " on page 149*.
  - Before you deploy the *EPS.msi* file, ensure that it is signed with a valid signature certificate.
- Reconnect Tool - Perform steps 1 to 4 for Windows in the *Reconnect Tool* topic and then do one of these steps to use the Reconnect tool:
  - Sign the *reconnect_utility.exe* file with your certificate and then continue with step 5 for Windows in the *Reconnect Tool* topic.
  - Run the *reconnect_utility.exe* file.

    It creates the **reconnect_tool** folder.

    a. Transfer the **reconnect_tool** folder to the endpoints.

    b. On the endpoint, open the **reconnect_tool** folder, and run the *ReRegister.exe* file.

Remote Access VPN

The Remote Access VPN component is a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel.

For more information, see the Endpoint Security clients homepage for your client version.

Access Zones

Access Zones lets you create security zones for use in Firewall. Configure Access Zones before configuring Firewall.

There are two predefined Access Zones:

- The **Internet Zone**
- The **Trusted Zone**

Network locations not placed in the **Trusted Zone** automatically belong to the **Internet Zone**.

Note:?Access Zones rules are computer-centric (and not user-centric).

Trusted Zone

The Trusted Zone contains network objects that are trusted. Configure the Trusted Zone to include only those network objects with which your programs must interact.

Note - Objects not placed in the **Trusted Zone** are placed automatically in the **Internet Zone**

SmartEndpoint contains an initial Access Zones policy. In the initial policy, these network elements are included in the Trusted Zone:

- **All_Internet**

  This object represents all legal IP addresses. In the initial policy, all IP addresses on the Internet are trusted. However, the Access Zones policy is not a policy that is enforced by itself but only as a component of the Firewall policy.

- **LocalMachine_Loopback**

  Endpoint computer's loopback address: 127.0.0.1. The Endpoint must always have access to its own loopback address.

Note - Endpoint users must not run software that changes or hides the local loopback address, for example personal proxies that enable anonymous internet surfing.

Objects in the Trusted Zone

Think about adding these objects to your Trusted Zone:

- Remote host computers accessed by your programs (if not included in the subnet definitions for the corporate network)
- Corporate WANs accessed by your programs
- Endpoint Security Management Server
- Domain name servers
- Mail servers
- Domain controllers
- File servers
- Print servers
- VPN Security Gateway address range
- Internet gateways
- Local subnets

- Security servers (for example, RADIUS, TACACS, or ACE servers)
- Other IP addresses or IP ranges, to which access is allowed or denied.

Changing the Access Zones Policy

The main component of the Access Zones policy rule is the definition of the Trusted Zone. All objects that are not in the Trusted Zone are automatically in the Internet Zone. If necessary, you can create new Trusted Zone objects to use in different policy rules

You can add and remove network objects from a Trusted Zone.

Note - A computer can have only one Trusted Zone. This means that if the Access Zones policy has more than one rule, and more than one Trusted Zone applies to a computer, only the last Trusted Zone is enforced.

To define the Trusted Zone:

1. In the **Policy** tab > **Access Zones** rule, double click **Corporate Trusted Zones** or right-click it and select **Edit Shared Action**.

   The **Edit Properties - Access Zones** window opens.

2. To *add* an existing object to the **Trusted Zone Locations** list:
   - Select a network object from **Available Network Objects**.
   - Click **Add**.
3. To *remove* an existing object:
   - Select the network object from the list
   - Click the **Remove** arrow
4. To *delete* an existing object, select the object and click **Delete**.
5. To *create* a new Network Object, click **New**.

   The **Select New Object Type** window opens.

   a. Select an object type from the list.

   b. Click **OK**.

   The **Properties** window for the selected object opens.

   c. Enter the required data.
6. Click **OK**.

To create a new Trusted Zone object:

1. In the **Policy** tab > **Access Zones** rule, double click **Corporate Trusted Zones** or right-click it and select **Edit Properties**.

   The **Properties** window opens.

2. In the **Select action** field, select **New**.
3. Edit the **Name** and **Description** of the Zone.
4. Click **OK**.
5. Edit the network locations in the zone as described in the procedure above.

Network Objects

Access Zones are made up of network objects. You define network objects by specifying one or more:

- Host
- IP address range
- Network
- Site

Create network objects for areas that programs must have access to, or areas that programs must be prevented from accessing.

Define objects for each policy or define objects before you create a policy. After defining an object, the object can be reused in other policies.

The same Network Objects and Services are used throughout the SmartEndpoint and in SmartConsole. When you create a new object, it is also available in SmartConsole. If you change an object in the SmartEndpoint or SmartConsole, it is changed everywhere that the object is used.

Note - The Trusted Zone and the Internet Zone can also be used as objects in a Firewall policy. These objects are resolved dynamically by the client based on Access Zones policy assignment to the client.

Configuring a Host as a Network Object

Enter data that defines the network object:

Object Information	Description
Name	A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
IP Address	The IP address of the host you want to use as a network object.
Color	Select a color to be used for the icon for this network object.
Comment	A description of the network object.

Configuring an Address Range as a Network Object

Enter data that defines the network object:

Object Information	Description
Name	A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
First IP Address / Last IP Address	The first and last IP addresses for the network object.
Color	Select a color to be used for the icon for this network object.
Comment	A description of the network object.

Configuring a Network as a Network Object

Enter data that defines the network object:

Object Information	Description
Name	A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
Network Address	The network address you want to use as a network object.
Net Mask	The net mask.
Color	Select a color to be used for the icon for this network object.
Comment	A description of the network object.

Configuring a Site as a Network Object

Enter data that defines the network object:

Rule Condition	Description
Name	A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.

Rule Condition	Description
Host Name	The full LDAP name of the host of the site you want to use as a network object. For example, hostname.acme.com.
Color	Select a color to be used for the icon for this network object.
Comment	Enter a description of the network object.

Configuring a Group as a Network Object

1. Enter data that defines the network object.
2. Select from the **Available Objects** column, or create new objects.

Fields:

Rule Condition	Description
Name	A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
Color	Select a color to be used for the icon for this network object.
Comment	Enter a description of the network object.

Configuring a Site Group as a Network Object

1. Enter data that defines the network object:

Rule Condition	Description
Name	A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
Color	Select a color to be used for the icon for this network object.
Comment	Enter a description of the network object.

2. Select an object from the **Available Objects** column, or create a new object of the type:

- Site
- Site Group

Remote Help

Users can be denied access to their Full Disk Encryption-protected computers or Media Encryption & Port Protection-protected devices for many different reasons. They might have forgotten their password or entered the incorrect password too many time. In the worst case scenario, a hacker might have tried access the computer or device.

Remote Help can help users in these types of situations. The user contacts the Help Desk or administrator and follows the recovery procedure.

Note - An Endpoint Security administrator can give Remote Help only if you enable Remote Help in the OneCheck User Settings policy.

Administrators can supply Remote Help through SmartEndpoint or through an online web portal.

- To use the SmartEndpoint - Select **Tools > Remote Help**
- To use the web portal - Go to `https://<Endpoint Security Management Server IP>/webrh`

There are two types of Full Disk Encryption Remote Help:

- One Time Login - One Time Login lets users access Remote Help using an assumed identity for one session, without resetting the password. Users who lose their Smart Cards must use this option.
- Remote password change - This option is applicable for users with fixed passwords who are locked out.

  For USB storage devices protected by Media Encryption & Port Protection policies, only remote password change is available

Web Remote Help

Administrators can use the built in Remote Help or online portal on the Endpoint Security Management Server, or create a dedicated server for the online web portal.

Administrators can authenticate to the web portal with these authentication methods:

- Check Point Password login (default)- Configure this in SmartEndpoint
- Active Directory Password - See *"Configuring SSL Support for AD Authentication" on page 433*
- Dynamic Token
- RADIUS or TACACS+ Authentication Server

Turning on Web Remote Help on Endpoint Security Management Server

You must turn on the Web Remote Help in SmartEndpoint before you can use it.

To turn on the Web Remote Help:

1. In SmartEndpoint, go to **Manage > Endpoint Servers**.

   The **Endpoint Servers** window opens.
2. Double-click on the name of a server in the list.
3. Select **Endpoint Remote Help Server**.
4. Click **Next**.
5. Install Database.

When you turn on or turn off the Web Remote Help, the Endpoint Security Management Server restarts and all connections with client computers and SmartEndpoint sessions get disconnected.

Configuring the Length of the Remote Help Response

Administrators can configure how many characters are in the Remote Help response that users must enter. The default length is 30 characters.

To change the length of the Remote Help response:

1. In the **Policy tab**, **Full Disk Encryption** rule, double-click the **Pre-boot Protection** action.
2. In the **Pre-boot Protection Properties** window, click **Advanced Pre-boot Settings**.

3. In the **Advanced Pre-boot Settings** window, **Remote Help** area, select a **Remote Help response length**.
4. Click **OK**.
5. Click **OK**.
6. Install policy.

Logging into Web Remote Help portal

You can log into Web Remote Help portal using one of these methods:

- Password Login
- Token Login

Password Login is the default method and shows when you first connect to the portal. The link in the right bottom corner of the Endpoint Security Web Remote Help window lets you toggle between the two login methods.

To login using Password Login method:

1. Enter a **User Name** and select a domain name from the **Domains** list.

   Notes -

   - You can set the user name in UPN format, for example: *UserName@example.com*
   - Domain name for the internal users is *internal-users*
2. Enter the **Password**.
3. Click **Log In**.

To login using Token Login method:

1. Enter a **User Name** and select a domain name from the **Domains** list.

   Notes -
   - You can set the user name in UPN format, for example: *UserName@ExampleCompany.com*
   - Domain name for the internal users is *internal-users*
2. Click **Next**.
3. Enter the **Challenge** string into your token.
4. Enter the **Response** generated by the *X.99 Token*.
5. Click **Login**.

Configuring a Standalone Web Remote Help Server

You can use the built in Remote Help or online portal on the Endpoint Security Management Server, or create a dedicated, standalone server for the online web portal.

To configure a standalone Remote Help Server:

1. In SmartEndpoint, go to Manage > Endpoint Servers.

   The Endpoint Server window opens.
2. Click **New**.
3. Select an Endpoint Security Management Server.
4. In the window that opens, select **Endpoint Security Management Server**.
5. Enter Server Name and IP Address.
6. Select a color (optional).
7. Enter a comment (optional).
8. Click **Next**.
9. Create SIC trust between the Primary Endpoint Security Management Server and the Remote Help sever:
   a. Enter the same SIC Activation Key as the one you entered in the Check Point Configuration Tool.
   b. Click **Initialize** to create a state of trust between the Endpoint Security Management Servers.
   c. If trust creation fails, click **Test SIC Status** to see troubleshooting instructions.
   d. If you have to reset the SIC, click **Reset**, reset the SIC on the Remote Help server, then click **Initialize**.
   e. Click **Next**.
10. Install Database on all servers.

Managing Web Remote Help Accounts

You can do these web Remote Help account management actions:

- Add a web Remote Help account

  Disable a Remote Help account
- Delete a web Remote Help account

- Edit a web Remote Help account
- Search for an existing web Remote Help account

Adding a Web Remote Help Account

1. In SmartEndpoint, go to **Manage > Web Remote Help Accounts**.

   The **Web Remote Help Accounts** window opens.

2. Click **New**.

   The **Web Remote Help Account** wizard opens.

3. Select a **User type**:
   - **Existing User/Group** - AD user or group
   - **Local User** - Check Point user
4. Click **Next**.
5. Configure login credentials:

User type & Authentication	Credentials
Existing user with AD authentication	a. In the **User/Group Name** field, select the user from the drop down list, or browse the Active directory (AD) tree to select a user. Alternatively, enter the name of the user from the AD (auto-complete field). b. In **Authentication credentials**, select **Active Directory credentials**.
Existing user with Token authentication	a. In the **User/Group Name** field, select the user from the drop down list, or browse the AD tree to select a user. Alternatively, enter the name of the user from the AD (auto-complete field). b. In **Authentication credentials**, select **Token**. c. Click **Select**. d. Select a token. e. Click **OK**.

User type & Authentication	Credentials
Existing User with RADIUS or TACACS+ Authentication	a. In the **User/Group Name** field, select the user from the drop down list, or browse the AD tree to select a user. Alternatively, enter the name of the user from the AD (auto-complete field). b. In **Authentication credentials**, select **Authentication Server**. c. Click **Select**. d. In the **Authentication Servers** window, Click **Add**. e. In the **Create New Authentication Server** window, enter the **Server Name**. It can be any name. f. Enter the **IPv4 Address** or **IPv6 Address** of the RADIUS or TACACS+ server. If the IPv4 or IPv6 address are not known or are dynamic, enter the **Domain Name** (for example radius.example.com). g. Select the Authentication Type. Either **RADIUS** or **TACACS+**

User type & Authentication	Credentials
	h. Enter the **Port** number. If not specified, the default port are used. ■ *RADIUS*: By default, the Endpoint Security Management Server listens for RADIUS traffic on UDP port 1812. This is the standard port for RADIUS authentication, as defined by the IETF in RFCs 2865 and 2866. However, by default, many access servers use ports 1645 for authentication requests. ■ *TACACS+*: By default, the Endpoint Security Management Server listens for TACACS traffic on TCP port 49. TACACS is defined in RFC 1492, and uses either TCP or UDP port 49 by default. i. In the **Secret Key** field, enter the secret key j. Click OK.
Local user with fixed password authentication	a. In the **Logon Name** field, enter the login name of a user. b. In **Authentication credentials**, enter a **Password**.
Local user with Token authentication	a. In the **Logon Name** field, enter the login name of a user. b. In **Authentication credentials**, select **Token**. c. Click **Select**. d. Select a token. e. Click **OK**.

User type & Authentication	Credentials
AD Group/OU with AD Authentication	a. In the **User/Group Name** field, select the group from the drop down list, or browse the AD tree to select a group. Alternatively, enter the name of a group from the AD (auto-complete field). b. In **Authentication credentials**, select **Active Directory credentials**. **Note** - Token authentication is not supported for AD Group/OU.

6. Click **Next**.
7. Set the expiration date (optional):
   a. Select **Expiration**.
   b. Select a **Start Date**.
   c. Select an **Expiration Date**.
8. Set the location, if necessary:
   a. In the **Account Details** section, click **Add**.
   b. Enter a location or select one from the list.
9. Click **Finish**.

Disabling the Web Remote Help account:

Select **Disable remote help account**. When you create a new account, it is enabled by default.

Editing a Web Remote Help Account

1. In SmartEndpoint, go to **Manage > Web Remote Help Accounts**.

   The **Web Remote Help Accounts** window opens.
2. Select an existing account from the list.
3. Click **Edit**.

   The **Edit Account** window opens.
4. Change the configuration as necessary.

Note - you cannot change the **User Name** of an existing account.

Deleting a Web Remote Help Account

1. In SmartEndpoint, go to **Manage > Web Remote Help Accounts**.

   The **Web Remote Help Accounts** window opens.
2. Select an existing account from the list.
3. Click **Delete**.
4. Click **OK**.

Searching for an Existing Web Remote Help Account

1. In SmartEndpoint, go to **Manage > Web Remote Help Accounts**.

   The **Web Remote Help Accounts** window opens.
2. In the search box, enter in the name of an account.

   List of results shows.

Configuring SSL Support for AD Authentication

To use Remote Help with AD password, it is necessary for the Remote Help server to connect to the domain controller with SSL.

To configure SSL Support:

1. Get an SSL certificate from your Domain Controller.
2. Import the SSL certificate to the Endpoint Security Management Server. See sk84620 for how to install the Domain Controller certificate on the Remote Help server.
3. Run this CLI command on the Endpoint Security Management Server to activate the SSL connection:

   ```
   $UEPMDIR/system/install/wrhAuthConfig
   ```

Note - Web Remote Help works with LDAPS or LDAP authentication only. Mixed mode is not supported.

Giving Remote Help to Full Disk Encryption Users

Use this challenge/response procedure to give access to users who are locked out of their Full Disk Encryption protected computers.

To give Full Disk Encryption Remote Help assistance from the SmartEndpoint:

1. Select **Tools** > **Remote Help** > **User Logon Preboot Remote Help**.

   The **User Logon Preboot Remote Help** window opens.

2. Select the type of assistance the end-user needs:

   a. **One Time Login** - Gives access as an assumed identity for one session without resetting the password.

   b. **Remote password change** - This option is for users who have forgotten their fixed passwords.

3. In the **User Name** field, click **Browse** and select the user in the **Select a Node** window.

4. Select the locked computer in the **Device Name** list.

5. Click **Generate Response**.

6. Tell the user to enter the **Response One (to user)** text string in the Remote Help window on the locked computer.

   The endpoint computer shows a challenge code.

7. In the **Challenge (from user)** field, enter the challenge code that the user gives you.

8. Click **Generate Response**.

   Remote Help authenticates the challenge code and generates a response code.

9. Tell the user to enter the **Response Two (to user)** text string in the Remote Help window on the locked computer.

10. Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.

To give Full Disk Encryption Remote Help assistance from the web portal:

1. Go to **https://<IP Address of Endpoint Security Management Server>/webrh**.

2. Enter your **User Name** and **Password** to log in to the portal. Administrators must have permission to provide Remote Help.

3. Select **FDE**.

4. Select the type of assistance the end-user needs:
    a. **One Time Login** - Gives access as an assumed identity for one session without resetting the password.
    b. **Remote password change** - This option is for users who have forgotten their fixed passwords.
5. In the **User Name** enter the User's name.
6. Select the locked computer in the **Device Name** list.
7. Click **Get Response One**.
8. Tell the user to enter the **Response One (to user)** text string in the Remote Help window on the locked computer.

    The endpoint computer shows a challenge code.
9. In the **Challenge (from user)** field, enter the challenge code that the user gives you.
10. Click **Get Response Two**.

    Remote Help authenticates the challenge code and generates a response code.
11. Tell the user to enter the **Response Two (to user)** text string in the Remote Help window on the locked computer.
12. Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.

Media Encryption & Port Protection Remote Help Workflow

Media Encryption & Port Protection lets administrators recover removable media passwords remotely using a challenge/response procedure. Always make sure that the person requesting Remote Help is an authorized user of the storage device before you give assistance.

To recover a Media Encryption & Port Protection password with Remote Help assistance from the SmartEndpoint:

1. Select **Tools** > **Remote Help** > **Media Encryption Remote Help**.

   The **Media Encryption & Port Protection Remote Help** window opens.

2. In the **User Logon Name** field, select the user.
3. In the **Challenge** field, enter the challenge code that the user gives you. Users get the **Challenge** from the Endpoint Security client.
4. Click **Generate Response**.

   Media Encryption & Port Protection authenticates the challenge code and generates a response code.

5. Give the response code to the user.
6. Make sure that the user can access the storage device successfully.

To recover a Media Encryption & Port Protection password with Remote Help assistance from the web portal:

1. Go to `https://<IP Address of Endpoint Security Management Server>/webrh`.
2. Enter your **User Name** and **Password** to log in to the portal. Administrators must have permission to give Remote Help.
3. Select **ME**.
4. In the **User Name** field, enter the name of the user.
5. In the **Challenge** field, enter the challenge code that the user gives you. Users get the **Challenge** from the Endpoint Security client.
6. Click **Generate Response**.

   Media Encryption & Port Protection authenticates the challenge code and generates a response code.

7. Give the response code to the user.
8. Make sure that the user can access the storage device successfully.

Disabling Remote Help

To disable Remote Help:

1. In the **Media Encryption & Port Protection Policy** window, in the **Encrypt Removable Media** area, click **Advanced Settings**.

   The **Media Encryption** page opens.

2. In the **Offline Mode Settings** expand the **Advanced Settings area**.

3. Clear the **Allow users to recover their password using remote help** option.

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 create a new Pre-boot user for User-bound Remote Help:

1. Use the procedure in *"Managing Authorized Pre-boot Users and Nodes" on page 270*.
2. In the **Account Details** window, select **Do not use device information for Full Disk Encryption Remote Help**.

Uninstalling the Endpoint Security Client Using Challenge-Response

You can allow a user to uninstall the Endpoint Security client on their remote Windows computer without giving the client uninstall password to the user. A challenge-response procedure validates the identity of the user on the remote computer.

Prerequisite for uninstalling using Challenge-Response:

The *administrator* configures the **Client Setting** policy one-time only, for all users:

1. In SmartEndpoint click the **Policy** tab.
2. In the **Client Settings** policy rule, in the **Actions** column, double-click **Default installation and upgrade settings**.
3. Select **Uninstall client using challenge-response** to allow users to uninstall their Endpoint Security clients using a challenge-response procedure.
4. Set the number of digits of the **Response length**. The default setting is *30 digits (High Security)*.

To allow a user to uninstall their Endpoint Security client using Challenge-Response:

1. The *user* starts the process to uninstall the Endpoint Security client:
    a. On the Windows computer, go to the **Add or remove programs** system setting, select the Endpoint Security, and click **Uninstall**.

    A **Check Point Endpoint Security** challenge-response window opens. The window has a **Challenge** field that contains a number with many digits, and a **Response** field that is blank.

    b. Give the **Challenge** number to the administrator. This can be by phone, text message, email, or in some other way.
2. The *administrator* generates a Response and gives it to the user:
    a. In the SmartEndpoint main **Menu**, select **Tools** > **Remote Help** > **Client Uninstall Remote Help**.

    The **Client Uninstall Remote Help** window opens.

    b. In **User Logon Name**, select the name of the user who wants to uninstall the Endpoint Security client.

    c. In **User Device**, select the computer of the user.

    d. In **Challenge from user**, type the challenge number that the user gave you.

e. Click **Generate Response**.

f. Give the **Response** number to the user. This can be by phone, text message, email, or in some other way.

3. The *user* uninstalls the Endpoint Security client:

a. Type the **Response** number into the **Check Point Endpoint Security** challenge-response window.

b. Uninstall the Endpoint Security client.

Offline Mode

Offline Mode lets users get policies and updates from a shared folder, without a connection to an Endpoint Security server. Policies for the following Endpoint Security client components are supported in Offline Mode:

- Full Disk Encryption
- OneCheck User Settings
- Client Settings

Configuring Offline Mode

Manage the offline policies for the Endpoint Security client components that are supported in Offline Mode 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.

1. **Create a new Offline Group and configure the sub-paths and settings**

   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:

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

      The **New Offline Group** wizard opens

   b. 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 and HTTPS paths are only supported when the WebDAV extension is enabled on the web server.
      - **Description** (optional) - Helpful information about the group or policies

   c. Click **Sub-paths**.

      The Sub-path Settings window opens.

d. 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.

e. Click **OK**.

f. 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.

g. Click **Next** to configure the Policies for the group.

2. **Configure a Policy for each Component of the Offline Group**

Configure a Policy for each Endpoint Security client component:

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 use

  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.

OneCheck User Settings Policy

- Continue with the **New Offline Group** wizard or click **OneCheck User Settings** to configure the OneCheck User Settings policy settings for the group.

  This policy will be the default **OneCheck User Settings** 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 **OneCheck User Settings** policy to them in SmartEndpoint. If users are acquired and not defined in SmartConsole, they always get the default policy.

Client Settings Policy

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

Completing the Wizard

- The Wizard shows the version and components 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.

Note - From the **Group Details** view, click **Pre-boot Users** to open:

- The **Authorized Pre-boot Users** list
- The **Blocked Pre-boot Users** list.

3. **Export the required 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.

Option	Description	Notes
Get Update Policy File	Exports a file with policy updates.	This file has CPPOL extension. You must put the CPPOL file in the **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.
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.	You must put the CPPOL file in the **Updates** folder.
Full Disk Encryption > Get Revert Pre-boot to Policy Configuration File	Returns the computer to the regular Pre-boot policy.	You must put the CPPOL file in the **Updates** folder.
Deployment > Get Initial Package	Exports a complete MSI with the Offline Policy. This can be used for new client installation.	
Deployment > 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.	Put the CPPOL file in the configured Updates folder and put the MSI in the configured Upgrades folder.

Option	Description	Notes
Deployment > 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.	You must put the CPPOL file in the **Updates** folder. For best practices, see *"Moving from Offline to Online Mode" on page 453*

To export all offline administrators:

a. Right-click on an offline group and select **Get Offline Management File (cpomf)** or

b. Select multiple administrators in an Administrator OU under an offline group, right-click, and select **Get Offline Management File (cpomf)**.

To replace the 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.

a. In the **Users and Computers** tab, right-click on the Offline Group and select **Advanced > Get Install Policy File**.

b. Replace the installation policy located in the local **Work** folder on the client.

The **Work** folder with the policy is located in:

- On x64 client:

```
%PROGRAMFILES(X86)%\CheckPoint\Endpoint Security\Endpoint Common\Work\
```

- On x86 client:

```
%PROGRAMFILES%\CheckPoint\Endpoint Security\Endpoint Common\Work\
```

c. Reboot to continue the installation.

4. **Deploy the Packages**

Instruct users to install the packages from the sub-paths. Make sure they have the required access.

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.

- On x64 client:

  ```
  %PROGRAMFILES(X86)%\CheckPoint\Endpoint Security\Endpoint Common\Work\
  ```

- On x86 client:

  ```
  %PROGRAMFILES%\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:

Location	Required Permissions						
	Read	Write	List	Execute	Modify	Delete	Create
Update Directory	✓		✓	✓			✓
Recovery Files Directory	✓	✓	✓	✓	✓	✓	✓
Client Log Directory	✓	✓	✓	✓	✓	✓	✓

Creating Offline Administrators

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

To create offline administrators:

1. Open **SmartEndpoint**.
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.
   - **Remove User** - Removes an offline administrator. Select the administrator in the table.
4. Click **Import** to import the administrators.
5. Click **OK**.

Editing Pre-boot Users

To edit offline Pre-boot accounts:

1. From the **Users and Computers** tab, expand an **Offline Group** to see the users .
2. Right-click the user and select **User Authentication (OneCheck)** > **Pre-boot Authentication method**.
3. Select an **Authentication Method**.
4. Click **Change Password** or **User Certificates** to create a new password or upload certificates, as required for the authentication method.
5. Click **OK**.

To edit a deployment Pre-boot account:

1. From the **Users and Computers** tab, open **Offline Groups**.
2. Select the preboot user account
3. Select **Deployment Pre-boot User Details** and click **Edit**.

To create offline Pre-boot users

1. From the **Users and Computers** tab, select an offline group.
2. In **Group Details**, click **Edit**.

   The **Group Details** window opens.
3. Click **Pre-boot Users**.

   The **Pre-boot Users Details** window opens.
4. In the **Authorized Preboot Users** area, 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**.

In **Account Details** you can configure the type of use and expirations settings.

- **Regular User** (default)
  - **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.
- **Deployment User**
  - **Allow creating X Pre-boot accounts from this account** - You can use this account to create new offline Pre-boot accounts. After it creates the maximum numbers of accounts allowed, the account expires.
- **Expiration Settings**:
  - **The user will expire after X logins to Pre-boot**
  - **The user will be revoked after** the selected date.

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 assistance and disk recovery. It does not require access to the Endpoint Security Management Server.

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

Get the files from the Server Release information section of the Endpoint Security homepage.

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 *"Export the required packages" on page 445*

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 Assistance

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

- **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.

Selecting 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 un-encrypt 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.

Uninstalling Endpoint Security Using Challenge-Response in Offline Mode

You can allow a user to uninstall the Endpoint Security client on their remote Windows computer without giving the client uninstall password to the user. A challenge-response procedure validates the identity of the user on the remote computer.

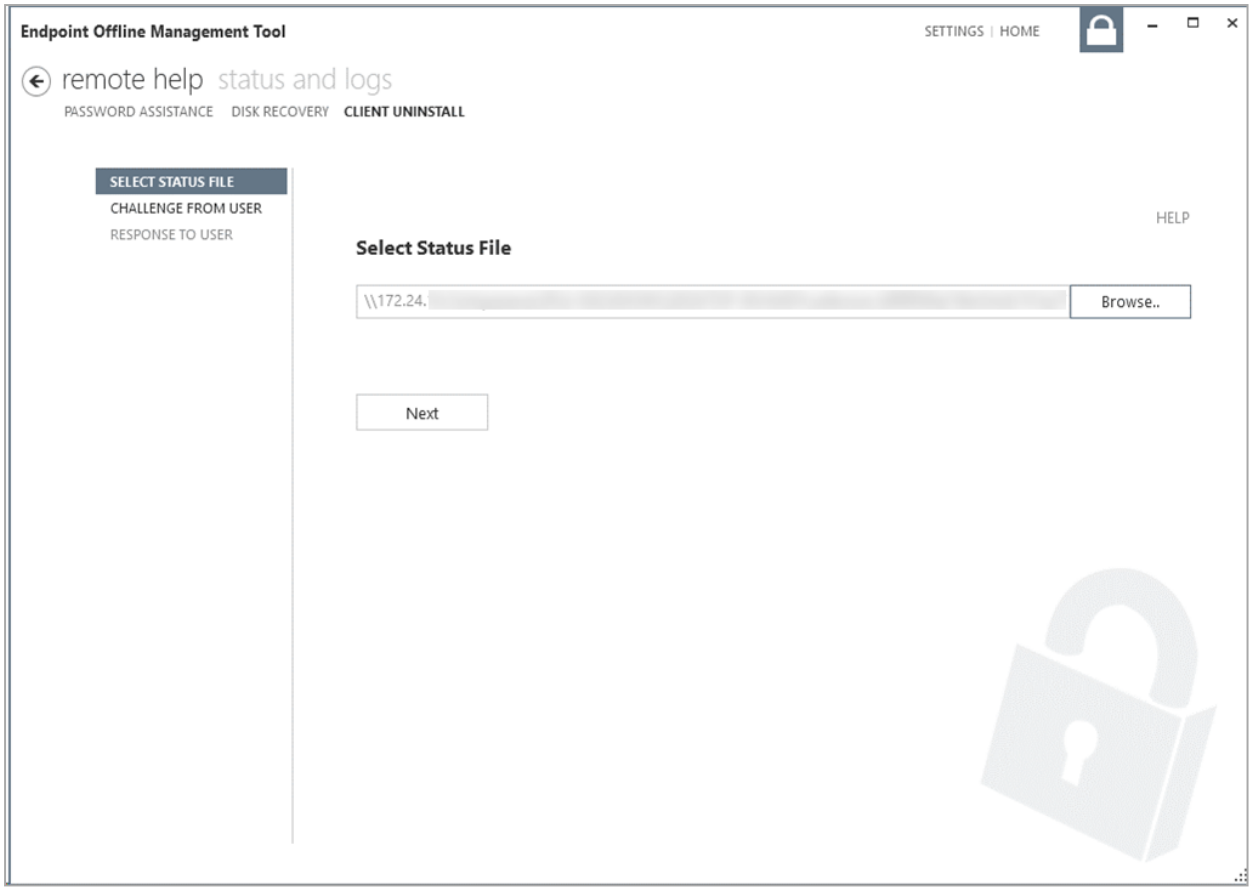
This is the procedure for Offline mode, using the Endpoint Offline Management Tool. This procedure is for environments where the clients do not have a connection to the Endpoint Security Server. If the clients do have a server connection, use the online procedure: *"Uninstalling the Endpoint Security Client Using Challenge-Response" on page 440*.

Configure the Client Setting policy one-time only, for all users:

1. In the SmartEndpoint **Users and Computers** tab, go to the **Offline Group**.
2. Click **Edit rule**.
3. In the **Client Settings**, edit the **Installation** rule, and select **Uninstall client using challenge-response**.
4. **Optional**: Set the number of digits of the **Response length**. The default setting is *30 digits (High Security)*.
5. In the main toolbar, click **Save rule**, and **Install the Policy**
6. In the offline group, click **Get Update Policy File** and save it to the **Updates** folder in the Offline location (the shared location where files for the Offline Group are stored).
7. After saving the policy file to **Updates** folder, the policy on the client is automatically updated. To update the policy immediately, tell the user to click **Update now** in the Endpoint Security client UI.

To allow a user to uninstall their Endpoint Security client using Challenge-Response:

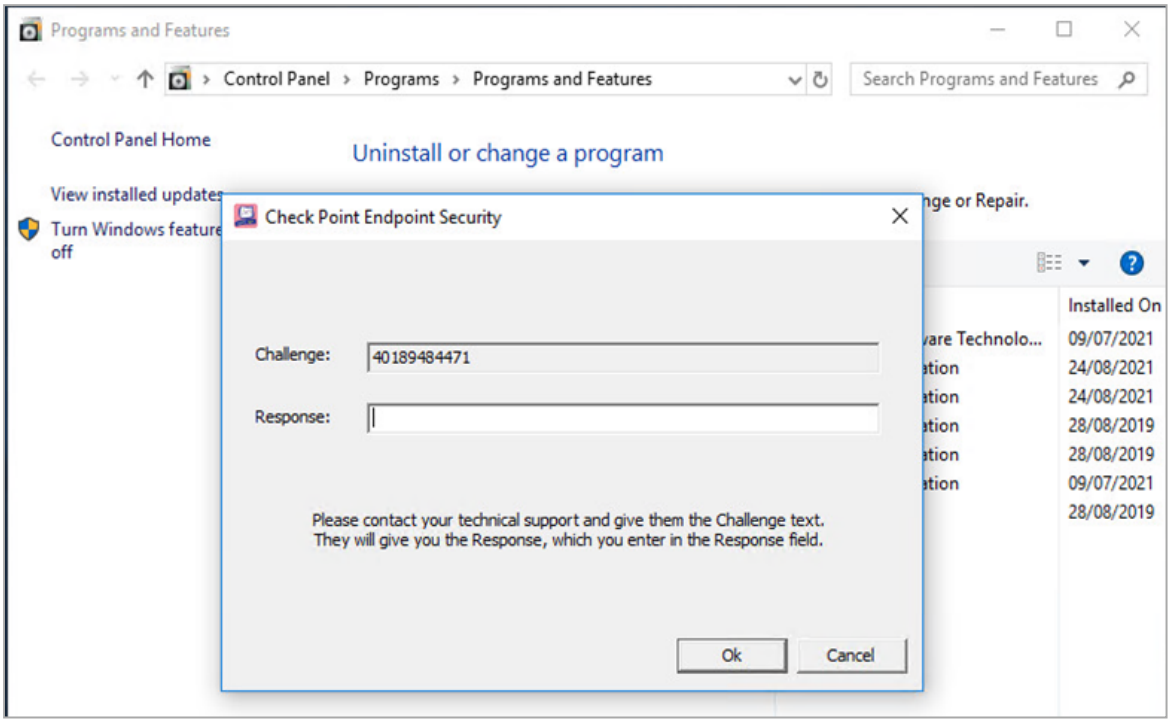
1. Open the Endpoint Offline Management Tool. See *"Logging In to the Offline Tool" on page 454*.
2. Click **CLIENT UNINSTALL**.



3. In **Select Status File**, select the `.cpsts` file of the client in the **Client Logs** folder in the Offline location.
4. Click **Next**.
5. Give these instructions to the *user*:

a. Start the process of uninstalling the Endpoint Security client. On the Windows computer, go to the **Add or remove programs** system setting, select the Endpoint Security client, and click **Uninstall**.

   A Check Point Endpoint Security challenge-response window opens. The window has a **Challenge** field that contains a number with many digits, and a **Response** field that is blank.



b. Give the **Challenge** number to the administrator. This can be by phone, text message, email, or in some other way

6. In the **CHALLENGE FROM USER** page of the Endpoint Offline Management Tool, in the **Challenge** field, type the number that the user gave you
7. Click **Next**.

   A Response number shows in **RESPONSE TO USER** page.
8. Give the **Response** number to the user. This can be by phone, text message, email, or in some other way
9. Give these instructions to the user:

   a. Uninstall the Endpoint Security client. Type the **Response** number into the **Check Point Endpoint Security** Challenge-Response window.

   b. Click **OK**.

      The Endpoint Security client is uninstalled.

c. If Full Disk Encryption (FDE) is installed, a popup window shows. Click **OK** to reboot the client computer. This decrypts the computer. Then, the Endpoint Security client is uninstalled.

Glossary