© 2014 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.
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.

Latest Documentation
The latest version of this document is at:
(http://supportcontent.checkpoint.com/documentation_download?ID=24673)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R77 home page (http://supportcontent.checkpoint.com/solutions?id=sk92965).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 November 2014</td>
<td>Added a step in Uninstalling the Client on Mac (&quot;Uninstalling the Client on Windows&quot; on page 53) and Uninstalling the Client on Windows (on page 53). New Discovered Devices (on page 25) report Updated License Enforcement (on page 14) Added Synchronizing MSI Files and Drivers (on page 73) Updated Backup and Restore Prerequisites (on page 82)</td>
</tr>
<tr>
<td>29 August 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security Management Server E80.50 on R77 Management Administration Guide).
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing and Configuring an Endpoint Policy Server</td>
<td>61</td>
</tr>
<tr>
<td>Configuration on R77 and R77.10 Management</td>
<td>61</td>
</tr>
<tr>
<td>How do Endpoint Policy Servers Work?</td>
<td>62</td>
</tr>
<tr>
<td>Configuring Policy Server Settings</td>
<td>63</td>
</tr>
<tr>
<td>Endpoint Policy Server Proximity Analysis</td>
<td>63</td>
</tr>
<tr>
<td>Enabling the Management Server to be an Endpoint Policy Server</td>
<td>64</td>
</tr>
<tr>
<td>Policy Server and Management Server Communication</td>
<td>65</td>
</tr>
<tr>
<td>Monitoring Endpoint Policy Server Activity</td>
<td>65</td>
</tr>
<tr>
<td><strong>Management High Availability</strong></td>
<td>67</td>
</tr>
<tr>
<td>Overview of Management High Availability</td>
<td>67</td>
</tr>
<tr>
<td>The High Availability Environment</td>
<td>67</td>
</tr>
<tr>
<td>Planning for Management High Availability</td>
<td>68</td>
</tr>
<tr>
<td>Configuring a Secondary Server in SmartDashboard</td>
<td>68</td>
</tr>
<tr>
<td>Failover</td>
<td>69</td>
</tr>
<tr>
<td>Changing a Server to Active or Standby</td>
<td>69</td>
</tr>
<tr>
<td>Understanding Server Status</td>
<td>69</td>
</tr>
<tr>
<td>Synchronizing Active and Standby Servers</td>
<td>70</td>
</tr>
<tr>
<td>Synchronization Procedures</td>
<td>70</td>
</tr>
<tr>
<td>Which Data is Synchronized</td>
<td>71</td>
</tr>
<tr>
<td>How Synchronization Works</td>
<td>71</td>
</tr>
<tr>
<td>Synchronization Status</td>
<td>72</td>
</tr>
<tr>
<td>Synchronization Troubleshooting</td>
<td>72</td>
</tr>
<tr>
<td>Environments with Endpoint Security</td>
<td>73</td>
</tr>
<tr>
<td>Manual Synchronization with Endpoint Security</td>
<td>73</td>
</tr>
<tr>
<td>Synchronizing MSI Files and Drivers</td>
<td>73</td>
</tr>
<tr>
<td>Updating the PAT Version on the Server</td>
<td>74</td>
</tr>
<tr>
<td>Synchronization with Endpoint Security</td>
<td>74</td>
</tr>
<tr>
<td>Disaster Recovery with High Availability</td>
<td>75</td>
</tr>
<tr>
<td>Recovery with a New Primary Server</td>
<td>75</td>
</tr>
<tr>
<td>Recovery by Promoting a Secondary Server</td>
<td>75</td>
</tr>
<tr>
<td>Promoting a Secondary Server to Primary</td>
<td>75</td>
</tr>
<tr>
<td><strong>Endpoint Security Active Directory Authentication</strong></td>
<td>77</td>
</tr>
<tr>
<td>Configuring Authentication</td>
<td>78</td>
</tr>
<tr>
<td>Configuring Active Directory for Authentication</td>
<td>78</td>
</tr>
<tr>
<td>Configuring Global Authentication</td>
<td>79</td>
</tr>
<tr>
<td>Troubleshooting Authentication in Server Logs</td>
<td>80</td>
</tr>
<tr>
<td>Troubleshooting Authentication in Client Logs</td>
<td>81</td>
</tr>
<tr>
<td><strong>Backup and Restore</strong></td>
<td>82</td>
</tr>
<tr>
<td>Overview of Backup and Restore</td>
<td>82</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>82</td>
</tr>
<tr>
<td>How to Back Up and Restore</td>
<td>82</td>
</tr>
<tr>
<td>Updating the PAT Version on the Server after Restore</td>
<td>83</td>
</tr>
<tr>
<td><strong>Full Disk Encryption Policy</strong></td>
<td>84</td>
</tr>
<tr>
<td>Overview of Full Disk Encryption</td>
<td>84</td>
</tr>
<tr>
<td>Full Disk Encryption Rule Actions</td>
<td>84</td>
</tr>
<tr>
<td>Disk Encryption</td>
<td>85</td>
</tr>
<tr>
<td>Authentication before Operating System (Pre-boot)</td>
<td>85</td>
</tr>
<tr>
<td>User Authorization before Encryption</td>
<td>89</td>
</tr>
<tr>
<td>OneCheck Logon</td>
<td>89</td>
</tr>
<tr>
<td>Full Disk Encryption Installation and Deployment</td>
<td>90</td>
</tr>
<tr>
<td>Client Requirements for Full Disk Encryption Deployment</td>
<td>91</td>
</tr>
<tr>
<td>Completing Full Disk Encryption Deployment on a Client</td>
<td>91</td>
</tr>
<tr>
<td>Stages of the Deployment Phase</td>
<td>91</td>
</tr>
<tr>
<td>Primary Full Disk Encryption Components</td>
<td>91</td>
</tr>
<tr>
<td>Full Disk Encryption Recovery</td>
<td>92</td>
</tr>
<tr>
<td>Full Recovery with Recovery Media</td>
<td>92</td>
</tr>
<tr>
<td>Dynamic Mount Utility</td>
<td>93</td>
</tr>
<tr>
<td>Upgrading Full Disk Encryption</td>
<td>93</td>
</tr>
<tr>
<td>Full Disk Encryption Troubleshooting</td>
<td>94</td>
</tr>
</tbody>
</table>
Chapter 1

Endpoint Security Introduction

In This Section:

- Overview of the System Architecture ................................................................. 9
- Software Blades .................................................................................................. 10
- Endpoint Security Services and Ports ................................................................. 11
- Centralized Organization of Users and Computers ............................................. 12
- Centralized Deployment ...................................................................................... 12
- Centralized Monitoring ....................................................................................... 12

Endpoint Security is a Management Software Blade in a Check Point Security Management Server. SmartEndpoint is the management console for Endpoint Security clients and their features.

**Endpoint Security Features:**

- One management console for endpoint security management
- Monitor your security status with a customizable, at-a-glance dashboard
- Quickly deploy the required protection for users using software-blade deployment rules
- Use pre-configured and customizable policies
- Easily change and report security policy changes at all levels of the organization
- Narrow-down to users and all their associated machines to investigate security status
- Enforce and resolve endpoint compliance issues before permitting access to the corporate network

**Overview of the System Architecture**

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

**Endpoint Security Management Server**

- **SmartEndpoint** - Check Point SmartConsole application to deploy, monitor and configure Endpoint Security clients and policies. Install on the **Endpoint Security Management Server** or on a computer that supports the client installation.

- **Endpoint Security Management Server** - Software Blade on Security Management Server with Endpoint Security policy management and databases. It communicates with endpoint clients to update their policies and protection data.

- **Endpoint Security Blades** - Software blades available on the Endpoint Security Management Server. You can install any or all of these blades on endpoint clients.

- **Endpoint Security Database** - Holds policies that enforce security on endpoint clients, holds user and computer objects, licensing, and Endpoint monitoring data.

- **Directory Scanner** - Software component that synchronizes the structure and contents of the **Active Directory** with the Endpoint Security policy database.
## Endpoint Security Clients

**Endpoint Security clients** - Application installed on end-user computers to monitor security status and enforce security policies.

**Endpoint Agent** - Endpoint Security software on client computers. It operates as a container for Software Blades deployed on the endpoint client and communicates with the Endpoint Security Management Server. (Endpoint Agent is also known as the Device Agent or DA)

**Endpoint Security Blades** - Software blades deployed on the endpoint client.

**Note** - When the term Endpoint Security Server is used, it refers to all Endpoint Security Servers in the environment. This includes Endpoint Security Management Servers or Endpoint Policy Servers.

## Software Blades

The Endpoint Security Management Server has rules in the policy for these security features.

<table>
<thead>
<tr>
<th>Blade</th>
<th>Rule</th>
<th>Description</th>
<th>Client OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption</td>
<td>OneCheck User Settings</td>
<td>Manages:</td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• How a Full Disk Encryption user logs in to the computer</td>
<td>Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• How failed logins are handled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access to remote help</td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>Full Disk Encryption</td>
<td>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.</td>
<td>Windows</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>Media Encryption &amp; Port Protection</td>
<td>Protects data stored on the computers by encrypting removable media devices and allowing tight control over computers’ ports (USB, Bluetooth, and so on).</td>
<td>Windows</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>Anti-Malware</td>
<td>Protects clients from known and unknown viruses, worms, Trojan horses, adware, and keystroke loggers.</td>
<td>Windows</td>
</tr>
<tr>
<td>Firewall</td>
<td>Access Zones</td>
<td>Defines the topology of the organizational network, separating it into Trusted and Internet domains.</td>
<td>Windows</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall</td>
<td>Blocks or allows network traffic based on attributes of network connections.</td>
<td>Windows</td>
</tr>
<tr>
<td>Firewall</td>
<td>Application Control</td>
<td>Controls network access on a per-application basis, letting you restrict application access by zone and direction.</td>
<td>Windows</td>
</tr>
<tr>
<td>Compliance</td>
<td>Compliance</td>
<td>Ensures that protected computers comply with your organization's requirements and allows you to assign different security levels according to the compliance state of the endpoint computer. For example, non-compliance can result in a remediation message, a warning, or restriction from the network.</td>
<td>Windows</td>
</tr>
</tbody>
</table>
VPN  | Remote Access VPN  | Remote Access VPN lets users connect remotely to a Check Point Security Gateway using IPSec.  | Windows, Mac

### Optional System Components

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

- Additional Endpoint Policy Servers that manage traffic from the Endpoint Security clients. This improves performance in large environments.
- One or more additional Endpoint Security Management Servers for High Availability. This makes sure that a backup server is always available for down time situations.

### Endpoint Security Services and Ports

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

**Important** - Make sure that these services and ports are not blocked by firewall rules. To do so, open SmartDashboard on the Endpoint Security Management Server and SmartEndpoint. Examine the rules on the Firewall tab.

Make sure to examine the hidden **Implied Rules**. You may have to configure the firewall rules to allow this traffic on these ports.

#### Services used by the client to communicate with the Endpoint Security Management Server:

<table>
<thead>
<tr>
<th>Client to Server Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy downloads</td>
<td>HTTP</td>
<td>TCP/80</td>
<td></td>
</tr>
<tr>
<td>Anti-Virus updates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client package</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint registration</td>
<td>HTTPS</td>
<td>TCP/443</td>
<td>Used to encrypt messages sent using the Endpoint Security Encrypted Protocol</td>
</tr>
<tr>
<td>New file encryption key retrieval</td>
<td>HTTPS</td>
<td>TCP/443</td>
<td></td>
</tr>
<tr>
<td>Synchronization request</td>
<td>ESP Encrypted</td>
<td>TCP/80</td>
<td>Heartbeat, communicates policy, status and compliance changes.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>ESP Encrypted</td>
<td>TCP/80</td>
<td></td>
</tr>
<tr>
<td>Log upload</td>
<td>ESP Encrypted</td>
<td>TCP/443</td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Recovery Data Upload</td>
<td>ESP Encrypted</td>
<td>TCP/443</td>
<td></td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection Key Exchange</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption User Acquisition &amp; User credentials</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SmartEndpoint uses SIC to reach the Endpoint Security Management Server:**

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Secure Internal Communication</td>
<td>SIC</td>
<td>TCP/18190</td>
<td></td>
</tr>
</tbody>
</table>
Before installing Endpoint Security Management Server, make sure these ports are not blocked:

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Reserved for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>8080</td>
<td>Communication between Security Management Server and Directory Scanner to Tomcat</td>
</tr>
<tr>
<td>8009</td>
<td>Communication between Apache and Tomcat</td>
</tr>
<tr>
<td>1080</td>
<td>SOCKS Proxy</td>
</tr>
</tbody>
</table>

Centralized Organization of Users and Computers

Manage your endpoint computers and users with the Endpoint Security Management Server.

**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. Endpoint Security Management server interface provides a granular view of all Endpoint Security policies, grouped by the blades they configure.

You create and assign policies to the root node of the organizational tree as a property of each Endpoint Security blade. 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 blade accordingly.

Centralized Deployment

Software Deployment in the Endpoint Security Management server lets you control specific blades and Endpoint Security versions installed on the protected end-user workstations.

Centralized Monitoring

Endpoint Security Management server provides reports for the whole system as well as individual users and computers. You can monitor Endpoint Security client connection status, compliance to security policy status, information about security events, and more.

- **General status reports** can be viewed in the Endpoint Security Management server.
- **Historical data for clients and servers** can be viewed in the SmartView Tracker application.
# Chapter 2

## Endpoint Security Licenses

In This Section:

- Endpoint Security Product Licenses ................................................................. 13
- Demo and Temporary Licenses ............................................................................ 14
- License Enforcement ........................................................................................... 14
- Getting Licenses .................................................................................................. 14
- Getting and Applying Contracts .......................................................................... 15
- License Status ..................................................................................................... 16

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

### Endpoint Security Product Licenses

This section describes the required Product licenses for Endpoint Security.

<table>
<thead>
<tr>
<th>License Type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container license</td>
<td>One license for each endpoint client (seat). This license is attached to the Endpoint Security Management Server.</td>
</tr>
<tr>
<td>Software Blade licenses</td>
<td>One license for each Endpoint Security Software Blade installed on an endpoint client (seat). The blade licenses include:</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption</td>
</tr>
<tr>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td></td>
<td>• Anti-Malware</td>
</tr>
<tr>
<td></td>
<td>• Network Protection - Bundle license that includes Endpoint Security Firewall, Compliance, Application Control, and Access Zones. This license automatically comes with the Container License.</td>
</tr>
<tr>
<td>Management license</td>
<td>A license for each Endpoint Security management server. The management license also includes these management blades:</td>
</tr>
<tr>
<td></td>
<td>• Management</td>
</tr>
<tr>
<td></td>
<td>• Logging &amp; Status</td>
</tr>
<tr>
<td></td>
<td>• User Directory</td>
</tr>
<tr>
<td>VPN License</td>
<td>A license for the VPN gateway that endpoint users connect to. You Install this license on the Security Management Server that manages VPN gateways. Do NOT install a VPN license on the Endpoint Security Management Server.</td>
</tr>
</tbody>
</table>
Demo and Temporary Licenses

These demo and trial Endpoint Security licenses are available:

<table>
<thead>
<tr>
<th>License type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demo License</td>
<td>A 15 day demo license is automatically installed with Check Point network security products. This license lets you use Security Gateways, the Security Management Server and all SmartConsole applications.</td>
</tr>
<tr>
<td>Trial License</td>
<td>A 30 day trial license is automatically installed when you install Endpoint Security. This license lets you use all Endpoint Security Blades for a limited number of endpoint client seats.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>An evaluation license is available for specified software blades for a specified number of seats.</td>
</tr>
<tr>
<td>Product</td>
<td>You must purchase a Product license for each Endpoint Security Software Blade running on a client. Licenses can be purchased as a Subscription, a contract that is renewed annually, or a one-time purchase.</td>
</tr>
</tbody>
</table>

License Enforcement

License activity conforms to these conditions:

- You can add Endpoint Security licenses as required using one of these methods:
  - SmartUpdate
  - The Gaia or SecurePlatform WebUI.
  - The cplic CLI command
  - The cpconfig command for Windows platforms
- 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 Blade licenses from a pool of available licenses.
- 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.
- When there is no container license, software blade registration is blocked (R77 Management only)

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 (http://usercenter.checkpoint.com).
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 Software Blade. If the macro string includes the -SUBSCR suffix, you must get and apply a contract for this feature ("Getting and Applying Contracts" on page 15).
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 and above.
   • 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:
   • SmartUpdate
   • The Gaia or SecurePlatform WebUI.
   • The cplic CLI command
   • The cpconfig command for Windows platforms

### 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. Open this file:
   \$CPDIR/conf/downloads/dl_prof_CNTCRMGR.xml
2. Change the <interval> value as necessary.
3. Run cpstop and cpstart.

**To apply a contract manually:**
1. Log in to Check Point User Center (http://usercenter.checkpoint.com).
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. Open SmartUpdate. (Start menu > Check Point > SmartUpdate)
7. 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.

### Configuring a Proxy for Internet Access

If the Endpoint Security Management Server requires a proxy to connect to the internet, configure the proxy details through a secure connection with the Endpoint Security Management Server, such as SSH.

**To configure a proxy for the Endpoint Security Management Server:**
1. Connect to the Endpoint Security Management Server through a secure connection, such as SSH.
2. Go to $UEFMDIR/engine/conf.
3. Edit the `local.properties` file:
   - Enter information for server IP and server port.
   - Delete the # signs.
4. Save the file.

**License Status**

You can see the status of container and blade 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
- Software Blades
- Seats in Use
- Total seats
- Percentage of total licenses in use
- Expiration date
- IP address of license host
Chapter 3

Using SmartEndpoint

In This Section:

Overview Tab .......................................................................................................... 17
Policy Tab ............................................................................................................... 18
Users and Computers Tab...................................................................................... 18
Reporting Tab ......................................................................................................... 18
Deployment Tab ...................................................................................................... 26
Client logging .......................................................................................................... 26
Finding Components in SmartEndpoint .................................................................. 27
Show/Hide Blades ................................................................................................... 27

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

To open SmartEndpoint:

Go to Start > All Programs > Check Point SmartConsole <version> > SmartEndpoint.

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 ("Alerts" on page 19) in Reporting tab > Alerts.

Security Status

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

1. Deployment Progress - Shows the progress of package deployment to endpoint computers
2. Blade Health Check - Shows which computers have installed Blades that are not running
3. Disk Encryption Status - Shows the status of Full Disk Encryption on endpoint computers
4. Anti-Malware Updates - Shows which endpoint computers have or are lacking current Anti-Malware signature updates
5. **Anti-Malware Protections** - Shows which endpoint computers are malware-free, have not been scanned or have malware problems

6. **Compliance Verification** - Shows which endpoint computers are compliant with the security policy and which are restricted or have pending warnings

Each category has:

- **A Trend tab**
  A line chart that shows the trend over time.

- **An 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 Blade. The wizard also lets you run the Directory Scanner ("Active Directory Scanner" on page 33) and configure Deployment rules ("Deploying the Software Blade Package" on page 41).

### Policy Tab

You define and manage policies for each Endpoint Security Software Blade on the Policy tab. An **Endpoint Security policy** is a collection of security rules that enforce protections on endpoint computers.

Rules are contained in a tabular grid with a different section for each Software Blade. Each section contains the rules applicable to that Software Blade. Each Software Blade has one default rule that applies to all endpoint computers and users that are not assigned to a different rule. You can change the default rule settings, but you cannot delete it.

### 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 **Save**.

### Reporting Tab

The Reporting tab includes many different types of Endpoint Security status reports. Each report shows a summary chart and list of monitoring information. You can sort and filter the monitoring information by different criteria.

**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 contains a chart that shows a graphical status summary of the select report item and an **Endpoint List** that shows all applicable users and computers. You can search and filter the list to see only
Using SmartEndpoint

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

**Endpoint List Section - Icons and Controls**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Enter a text string to search all columns and results that contain the string are shown.</td>
</tr>
<tr>
<td>Status:</td>
<td>Select a status to filter by. The options are based on the open report. Endpoints with that status are shown.</td>
</tr>
<tr>
<td>In:</td>
<td>Narrow the results to an OU, node or group in the organization. Click ... to select an item in the Select Node window.</td>
</tr>
<tr>
<td>or</td>
<td>Double click to open the selected user or computer.</td>
</tr>
<tr>
<td>Click</td>
<td>Click to see other options available. Some options are not available for all reports.</td>
</tr>
<tr>
<td>• Export to file</td>
<td>Export the report results to an XLS, HTML, or CSV file.</td>
</tr>
<tr>
<td>• Toggle chart percentage</td>
<td>Add and remove the percentages shown on the graph.</td>
</tr>
<tr>
<td>• Navigate To</td>
<td>Lets you navigate to specified users or computers.</td>
</tr>
<tr>
<td>• Anti-Malware</td>
<td>Run a Push Operations for Anti-Malware on the endpoint.</td>
</tr>
<tr>
<td>• Client Settings</td>
<td>Run a Push Operations for Client Settings on the endpoint.</td>
</tr>
<tr>
<td>• Add to virtual group</td>
<td>Add the selected objects to a virtual group.</td>
</tr>
</tbody>
</table>

**Alerts**

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

- Computers with Anti-Malware Problems
- Computers with Anti-Malware Update Errors
- Compliance problems
- Computers with some Software Blades not running or status unknown
- Computers with failed deployments
- Computers with encryption problems
- Computer not scanned by Anti-Malware
- Computers with Security Verification warnings

The **Security Picture** feature automatically sends email alerts to administrators when the number of endpoints with security violations exceeds a predefined threshold. The top section of the pane shows the status of each violation type, including the quantity and percentage of endpoint computers in violation. Also shown are the threshold conditions for sending and stopping alerts.

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 these types of messages:

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

**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 the Email Server

You must configure your email server settings before Security Picture can send alert email messages. These 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. If email server authentication is necessary, select **User authentication is required**. Configure these parameters:
   - **Port** - Email server port number (default = 25)
   - **User Name**
   - **Password**
4. Click **Check Connectivity** to make sure that you can successfully access the email server. If the verification fails, correct parameter errors or resolve network connectivity issues.
**Troubleshooting issues with email alerts**

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.

**Endpoint Security Analysis Report**

The **Endpoint Security Analysis Report** is a summary of all Endpoint Security clients in the environment. Each client sends information to the server one time each day and the information is summarized by the server hourly.

The **Endpoint Security Analysis Report** includes:

- General data loss risk and computers with the highest risk of data loss.
- General unauthorized access risk and computers with the highest risk of unauthorized access.
- General threat risk and computers with the highest risk of threats.

The report is generated if the **Generate Endpoint Security Analysis Report** action is selected in **Policy tab > Compliance** rules. The action is the same in all Compliance rules.

**Push Operations**

Push Operations are operations that the Endpoint Security Management Server pushes directly to client computers with no policy installation required.

These Push Operations are available:

- **Anti-Malware**
  - **Scan for malware** - Run an Anti-Malware scan on the computer or computers, based on the configured settings.
  - **Update malware signatures** - Update malware signatures on the computer or computers, based on the configured settings.
  - **Temporarily restore files from quarantine** - Temporarily restores files from quarantine on the computer or computers, based on the configured settings.

- **Client Settings**
  - **Shut down computer** - Shut down the computer or computers based in the configured settings.
  - **Restart computer** - Shut down the computer or computers based in the configured settings.
  - **Collect client logs** - Collect logs from the computer or computers based in the configured settings.
    Logs are stores in a shared folder on the client computer.
  - **Repair client** - Repair the Endpoint Security client installation. This requires a computer restart.

From **Reporting tab > Push Operations** you can:

**In the top pane:**

- See all recent Push Operations activities, and their details. This includes: which objects were included in the operation, the status.
- Create new, Abort (stop), and Remove Push Operations.
- Click **Configure Defaults** to configure the default settings for a selected operation. These settings will apply each time you run Push Operations and do not configure different settings.

**In the Endpoint List:**

See the results of the operations on each endpoint.
You can also start Push Operations from everywhere in the SmartEndpoint where an object is shown. This includes reports in the Reporting tab and in the Users and Computers tab.

Starting Push Operations

To start Push Operations from an object in the SmartEndpoint:
1. Right-click the object (user or computer) and select Anti-Malware or Client Settings and then select an operation.
2. Click Yes to confirm that you want to do the operation.
3. Optional: Click Advanced Settings to use settings that are not the default.

To start Push Operations from Reporting > Push Operations:
1. In Reporting > Push Operations, click Create new.
2. Select Anti-Malware or Client Settings and then select an operation.
3. Click Next.
4. Select an OU, node, or computer to get the operation.
5. Click Next.
6. Configure the settings for the operation.
7. Click Next.
8. Click Finish.

Push Operations Settings

Click Configure Defaults to configure the default settings for a selected operation. These settings will apply each time you run Push Operations and do not configure different settings.

Select the operation to configure.

For each operation you can configure:

- **User Notification** - Are users notified about the operation and can they cancel or postpone it. The options are:
  - **Execute operation immediately** - Users cannot cancel or postpone it.
  - **Allow user to postpone or cancel operation** - Users can cancel or postpone it. Click Configure to configure the notification message that users see and in how many minutes the operation will occur.

- **Scheduling** - When does the operation occur. The options are:
  - **Execute operation immediately**
  - **Schedule operation for** - Enter a date and time when the operation will start.

- **Timeframe** - The Endpoint Security Management Server will send the operation to clients for the selected number of hours.

For Anti-Malware Push Operations, see Anti-Malware Policy Actions (on page 125) for more information.

Compliance

- **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 ("Configuring the "About to be Restricted" State." on page 60).
- **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 Software Blades for users and endpoint computers. You can use this report to see which blades 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**

You can select reports that show deployment status by:

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

For all Software Deployment reports, the available status categories are:

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

Hover 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 blade for endpoint clients.
- **Endpoint Package Versions** - Shows the installed version of Endpoint Agent for individual endpoint clients.

**Full Disk Encryption**

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)**

- **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**

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**

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 scanning status by Anti-Malware provider brand
- **Anti-Malware Scanned Date** - Shows status by the last scan date

**Licenses Report**

The Licenses Status Report shows the status of the container and blade 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 blade or the container. You can export license status information to a file.

To see license warnings, click Details.

**Custom Report**

This report type lets you create custom reports based on multiple monitoring criteria.

**To create a custom report:**
1. In the Reporting tab, select Custom Report.
2. In the Custom Report pane, click Choose monitoring criteria.
3. In the Custom Report window, use the buttons to add or remove monitoring criteria from the Selected Status list.
4. Click OK.
5. Use the Show Endpoints that box to show data that matches the selected criteria.
6. In the Endpoints List area, use the Status drop-down box to create a filter for endpoint computers that show in the list.

**Deployment Tab**

You use this tab to:

- Create Software 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**

These policies on the client upload logs to the Endpoint Security Management Server:

- Firewall
- Application Control
- Anti-Malware
- Compliance
- Full Disk Encryption
- Media Encryption and port protection
On the server, the logs are stored in the common log database, which is read by SmartView Tracker.

**Note** - The VPN blade uploads SCV logs to the VPN gateway.

Client logs are:
- Stored locally at:
  
  `C:\Documents and Settings\All Users\Application Data\CheckPoint\Endpoint Security\Logs`

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

- Uploaded according to the Common Client Policy to the Endpoint Security Management Server and viewable in SmartView Tracker.
- Client logs can be used for external audit requirements and internal trouble-shooting.


**Finding Components in SmartEndpoint**

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.**
   
   **Note** - Alternatively, right-click any user shown on the Reporting tab and select **Edit**.

**Show/Hide Blades**

You can choose which blades show in SmartEndpoint and which are hidden. By default, WebCheck is hidden and is only supported for environments that used WebCheck in an earlier release.

**To show or hide a blade in SmartEndpoint:**
1. **From the Menu icon, select Tools > Show/Hide Blades.**
2. **Click on a blade to see if it is Visible or Hidden.**
3. **Click the Visible or Hidden button to change the blade’s setting.**
4. **Click OK.**
Chapter 4

Users and Computers

In This Section:

Managing Users and Computers ................................................................. 28
Active Directory Scanner ............................................................................. 33
Endpoint Security Administrator Roles ....................................................... 36
Working with Virtual Groups .................................................................... 36

Managing 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.
- **The Blades Pane** - Shows the Software Blades and their status for the selected object. Select a Software Blade to see its rules and status.
- **The Rule and Status Pane** - Shows the rules and status for the selected Software Blade. 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 blade:

- 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 Software Blade (if applicable). For OUs and groups, the status section shows selected reports ("Reporting Tab" on page 18) for some blades.

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 Software Blade. You can click on a Software Blade to go to the detailed information pane for that blade.

- **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.
- **Software Blades** - Shows detailed rule and status information for each blade. For OUs and Groups detailed status reports ("Reporting Tab" on page 18) are shown.

### Changing Authentication Settings

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

- The Pre-boot authentication method ("Pre-boot Authentication Methods" on page 98) when the Full Disk Encryption Blade is active. The default authentication method is **Password**.
- Lock a user out ("Account Lock" on page 101) after a specified number unsuccessful login attempts from the Pre-boot screen.
- 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.
- **Reset Computer Data** ("Resetting a Computer" on page 32) - Remove licenses, Full Disk Encryption recovery data, Pre-boot settings, users and logs from the selected computer.
- **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.
- **View SmartLog logs** - See this object in logs.
- **Full Disk Encryption** - Opens a list of operations related to Full Disk Encryption.
  - **Authorize Pre-boot users** - Manually add users authorized who can login using the Full Disk Encryption Pre-boot screen.
  - **Authorize Pre-boot nodes** - Manually add computers on which authorized users can login using the Full Disk Encryption Pre-boot screen.
  - **Disable Pre-boot protection** - Temporarily disable Pre-boot login for the selected user or members of the selected OU or group.
- **Encryption recovery media** - Manually add users authorized to use recovery media to recover an encrypted disk.

- **Anti-Malware** - Opens a list of Push Operations related to Anti-Malware. Push Operations are operations that the Endpoint Security Management Server pushes directly to client computers with no policy installation required.

- **Scan for malware** - Run an Anti-Malware scan on the computer or computers, based on the configured settings.

- **Update malware signatures** - Update malware signatures on the computer or computers, based on the configured settings.

- **Temporarily restore files from quarantine** - Temporarily restores files from quarantine on the computer or computers, based on the configured settings.

- **Client Settings** - Opens a list of Push Operations related to Client Settings. Push Operations are operations that the Endpoint Security Management Server pushes directly to client computers with no policy installation required.

- **Shut down computer** - Shut down the computer or computers based on the configured settings.

- **Restart computer** - Shut down the computer or computers based on the configured settings.

- **Collect client logs** - Collect logs from the computer or computers based on the configured settings. Logs are stores in a shared folder on the client computer.

- **Repair client** - Repair the Endpoint Security client installation. This requires a computer restart.

- **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 Software Blade 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 blade. 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 **User Details** ("Using the Object Details Window" on page 28) window opens. You can see detailed information as well as rules and status information for each of the Software Blades. 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 blade in the **Blades** pane.
3. Click **Edit Rule**.
4. Do the steps in the **Edit Specific Rule** wizard.
   See the applicable Software Blade 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 Details ("Using the Object Details Window" on page 28) window opens. You can see detailed information as well as rules and status information for each of the Software Blades. 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 blade in the Blades pane.
3. Click Edit Rule.
4. Do the steps in the Edit Specific Rule wizard.
   See the applicable Software Blade 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 Software Blades. 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 blade in the Blades pane.
3. Click Edit Rule.
4. Do the steps in the Edit Specific Rule wizard.
   See the applicable Software Blade topics for configuration details.
5. On the SmartEndpoint toolbar, select File > Save.

Managing Users of a Computer

If the Full Disk Encryption blade 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.
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. For this to succeed, the user account related to each Directory Scanner instance requires read permissions to:

- The Active Directory path to be scanned.
- 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.

For more information, see the Microsoft Knowledge Base [http://support.microsoft.com/default.aspx?scid=kb;en-us;892806](http://support.microsoft.com/default.aspx?scid=kb;en-us;892806).

**Note** - When using multi-domain scanning, you must configure an Active Directory instance for each domain. A Directory Scanner instance has its own account, configured according to the requirements stated above.

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. You can configure multiple scanner instances to scan different domains or different OUs in the same domain.

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

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, mycompany.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.
   - **LDAP Path** - The LDAP Path is filled in automatically if the domain controller was resolved by the DNS server. Click the browse button to select an OU. If you do not select an OU, the full domain is scanned.
4. In the **Advanced** area:
   - **Domain Controller** - Select a Domain Controller. If the domain has DNS, this is filled in automatically.
   - **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.
     - **SSL Enabled** - Uses SSL Tunneling. You must have an SSL certificate installed on the Domain Controller.
- **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.

5. 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

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

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: Stronger authentication is required**

**Solution:**

- Try to connect with SSL with these steps:
  - a) Get an SSL certificate from your Domain Controller.
  - b) Import the SSL certificate to the Endpoint Security Management server. See sk84620 ([http://supportcontent.checkpoint.com/solutions?id=sk84620](http://supportcontent.checkpoint.com/solutions?id=sk84620)).
  - c) Make sure that SSL Enabled is selected for this Directory Scanner instance.

**Issue: Wrong SSL Port**

**Solution:**

Change the SSL port or disable SSL. You can do this in the configuration.

**Issue: Cannot connect to the domain controller**

**Solution:**

Make sure that an LDAP server is running on the LDAP path of the configured domain controller.

**Issue: SSL certificate is not installed**

**Solution:**

- 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:
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.

**Endpoint Security Administrator Roles**

Endpoint Security uses the Permissions Profiles configured in SmartDashboard to define administrator roles. Make sure that administrators have the permissions required to do their tasks.

**To define Endpoint Security administrator permission profiles:**
1. In SmartDashboard, select the Firewall tab.
2. Select **Manage Permissions Profiles**.
3. In the Permissions Profile window, double-click an existing profile or click **New**.
4. In the Permissions Profile Properties window, select **Customized** and click **Edit**.
5. In the Edit Permissions of Profile window, select the **Endpoint** branch.
6. Configure these administrator permissions as necessary:
7. Click **OK**.
8. Click **OK**.
9. Click **Close**.
10. Select **File > Save**.

**Working with Virtual Groups**

Virtual Groups let you manage groups of users and computers with SmartEndpoint. You can use Virtual Groups with Active Directory for added flexibility or as an alternative to Active Directory.

Objects can be members of more than one virtual group. Members of Active Directory OUs or groups can also be members of Virtual Groups.

The benefits of using Virtual Groups include:
- 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.

Virtual Groups work much like Active Directory. You can:
- Create groups and then add objects to the groups automatically or manually.
- Assign policies to virtual groups or users.
- Put objects into more than one group.
- Select which policies have priority for endpoints that belong to more than one virtual group.

**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. Afterwards you can move them between virtual groups manually.
Types of Virtual Group

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.

These predefined virtual groups are created with users and computers assigned to them automatically:

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

If you add objects to a virtual group with an installation package (*Adding Objects with an Installation Package* on page 38), the objects are not automatically put into these virtual groups. You must do so manually.

Basic Virtual Group Management

You work with virtual groups in the Virtual Groups branch of the Users and Computers tree. The virtual groups are located under the Virtual Group branch.

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

- 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.

To create a new virtual group:

1. In the Users and Computers tree, click Virtual Groups.
2. Right-click and select New Virtual Group.
3. In the New Virtual Group window:
   - Enter a name for the group.
   - Optional: Enter a Comment.
   - Select Virtual Group or Computer Group.
4. Click OK.

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.

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 Software 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 Group Objects

Virtual Group objects 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.
Chapter 5

Deploying Endpoint Security Clients

In This Section:

- Deployment Overview ............................................................................................. 39
- Deploying the Initial Client ...................................................................................... 40
- Deploying the Software Blade Package ................................................................. 41
- Working with Deployment Rules ............................................................................. 43
- Advanced Package Settings ................................................................................... 44
- Installing the Client Using the CLI ........................................................................... 45
- Initial Security Client Analysis ................................................................................. 46
- Deploying Mac Clients ............................................................................................ 46
- Upgrading Endpoint Security Clients ...................................................................... 47
- Upgrading Legacy Clients ....................................................................................... 49
- Troubleshooting the Installation .............................................................................. 51
- Uninstalling the Client on Windows......................................................................... 53
- Configuring Log Forwarding .................................................................................... 53

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

- For clients on Windows, you can use one of these deployment strategies:
  - **Automatic** (recommended) - Use Software 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 Overview ("Deployment Overview" on page 39)
  - **Manual** - Export Software Blade 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 Working with Software Blade Packages for Export ("Working with Software Blade Packages" on page 42).

- For clients on Mac, see Deploying Mac Clients (on page 46).

**Deployment Overview**

There are two different types of deployment packages that you must deploy to install endpoint clients:

- **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.

- **Software Blade Package**
  This package includes the specified Software Blades to be installed on the endpoint client. This can be distributed automatically with Software Deployment rules or manually with exported packages.

We recommend that you first deploy the Initial Client and make sure that the client can communicate with the Endpoint Security Management Server. You can then deploy the Software Blade package.

**Note** - Endpoint users must have administrator rights on their computers to install the packages. For Windows versions higher than XP, users must run the package with the Run as Administrator option.
Deploying the Initial Client

You can get the Initial Client from SmartEndpoint, the distribution media, or the homepage sk. 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.

There are two different types of Initial Client packages.

- For new client installations, use the **eps.msi** Initial Client.
- To upgrade existing clients with legacy password support, use the **PreUpgrade.exe** Initial Client.

The **PreUpgrade.exe** package unlocks legacy files using a predefined uninstallation password. It then continues to install the Initial Client package.

You can also install the initial client silently using third party **.msi** deployment software, such as AKA GPO, Symantec Altiris or other solutions.

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 **Software Deployment** tab.
2. Under **Initial Client**, click **Download**.
3. In the **Legacy Uninstall Password** window, click **Skip**.
   - If you are upgrading from a legacy Endpoint Security Management Server, see Upgrading Clients ("Upgrading Endpoint Security Clients" on page 47).
4. Optional: Select a Virtual Group destination.
5. In the **Browse for Folder** window, click **Make new Folder**.
   - Assign a folder name that describes the package contents, such as 'Initial Client.'
6. 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 distribution media:**

1. Create a folder for the Initial Client on your local computer.
2. On the distribution media, go to `windows\CPEPclnt\NEWDA`.
3. Copy **EPS.msi** to the folder.

**To get the Initial Client from the Support Center:**

1. Create a folder for the Initial Client on your local computer.
4. In the **Version** filter section, select E80.50.
5. Download **Endpoint Security E80.50 Server for Windows**.
6. In the ISO file, go to `windows\CPEPclnt\NEWDA`.
7. Copy **EPS.msi** to the folder.

Deploying the Initial Client to Endpoint Computers

You can use third-party deployment software, a shared network path, FTP, email or other method to deploy the Initial Client to endpoint clients. Users manually run the deployment package on their computers to install the Initial Client.
Deploying Endpoint Security Clients

Seeing the Deployment Status

To see the Software Blade deployment status:
1. Go to the Reporting tab.
2. Select Software Deployment from the tree.
3. Select one of the Software Deployment status reports.

Deploying the Software Blade Package

The Software Blade package contains the Software Blades to be installed on endpoint clients. Each Software Blade has one or more policies that define the security settings. You can configure the policies for the Software Blades before or after you deploy the Software Blade package. These are different Software Blade packages for 32 bit and 64 bit Windows platforms.

These default client packages are included with this release:

<table>
<thead>
<tr>
<th>Directory Name</th>
<th>Contains These Client Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master_FULL</td>
<td>32 Bit Full package including all Software Blades</td>
</tr>
<tr>
<td>Master_FULL_x64</td>
<td>64 Bit full package including all Software Blades</td>
</tr>
<tr>
<td>Master_FULL_NO_NP</td>
<td>32 bit Media Encryption &amp; Port Protection and Full Disk Encryption only.</td>
</tr>
<tr>
<td>Master_FULL_NO_NP_x64</td>
<td>64 bit Media Encryption &amp; Port Protection and Full Disk Encryption only.</td>
</tr>
<tr>
<td>NEWDA</td>
<td>32 bit Initial Client without any blades</td>
</tr>
</tbody>
</table>

You cannot distribute these packages using deployment rules.

The default package directories can be found in these paths:
- **Windows** - %fwdir%\conf\SMC_Files\uepm\msi
- **Gaia and SecurePlatform** - $FWDIR/conf/SMC_Files/uepm/msi

The standard Software Blade package names are:

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Endpoint Total Security</td>
<td>All Software Blades</td>
</tr>
<tr>
<td>Check Point Endpoint Disk and Media Security</td>
<td>Full Disk Encryption and Media Encryption &amp; Port Protection</td>
</tr>
</tbody>
</table>

You can create your own customized Software Blade packages as necessary. You can deploy Software Blade Packages to endpoint clients using these methods:

- **Software Deployment Rules** - Automatically installs the correct Software Blade package version (32 or 64 bit) on endpoint clients. You define deployment rules and manage deployments using SmartEndpoint.
  You can see the status of all deployments in the Reporting tab.

- **Exporting Packages** - You can export Software Blade packages from the Endpoint Security Management Server to endpoint clients using third party deployment software, a shared network path, email or other method.
  Make sure to install the correct package version (32 or 64 bit) on endpoint clients. If you try to install the incorrect package, the installation fails. You can only see the deployment status after the package is successfully installed.
Discovering Endpoint Security

**Working with Software Blade Packages**

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

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

**To create or change a package:**

1. In the **Deployment** tab, select **Packages for Export**.
2. To add a new package, click **Add**.
   - 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 **Upload**, to add more package versions to the repository.
5. Click the **Desktop Blades** and **Laptop Blades** cells and then select the Software Blades to include in the package.
6. In the **Settings** column:
   - Select a **Virtual Group** or **Computer Group** to receive the policy.
   - Define new Virtual Groups or Computer Groups
   - Add passwords for legacy Secure Access and Full Disk Encryption upgrades
   - Remove a selected group
   - If you defined a Remote Access VPN blade, 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
7. **If you are upgrading legacy Endpoint Security release:**
   - a) Double-click **Legacy Secure Access upgrade support** and/or **Legacy Full Disk Encryption EW upgrade support**.
   - b) Enter and confirm the applicable passwords.
8. In the **Software Deployment Rules** window, click **Save**.

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

**Defining the Default VPN Site**

You can configure each Software Blade package to connect to a default VPN site. You do this by changing the VPN site definition in the **Settings** cell.

By default, a new package uses the **No VPN site defined** setting.

**To define the default VPN site:**

1. Select a package. Make sure it includes Remote Access VPN in the **Desktop Blades** column.
2. In the **Settings** cell, double-click the VPN line.
   - This line can contain the **No VPN site defined** item or a predefined VPN site.
3. Select another VPN site from the list.
   - You can also click **Add** to create a new VPN site ("Defining a VPN Site" on page 44).
4. In the **Software Deployment Rules** window, click **Save**.
**Exporting Packages**

On Windows 8 and higher clients, you must install an exported package with **Run as administrator** selected. You cannot install it with a double-click.

1. In the **Packages for Export** window, select a package.
2. Click **Export Package**.
3. 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.
4. Click **OK**.
   The package **EPS.msi** and/or **PreUpgrade.exe** files are downloaded to the specified path. A different folder is automatically created for each option selected in step 3a.
5. Send the **EPS.msi** and **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.

**Working with Deployment Rules**

Software Deployment rules let you manage 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 Software Blades to groups of endpoint computers with different criteria, such as:

- Specified Organizational Units (OUs) and Active Directory nodes
- Specified Networks
- Specified computers and users
- 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 Software Blades. The Initial Client examines the endpoint computer version (32 or 64 bit) and installs the correct package.

**Creating New Deployment Rules**

1. Click the **Deployment** tab and select **Software Deployment Rules**.
2. Click **Create Rule**.
   The **Create Rule** wizard opens.
3. In the **Select Entities** window, select an entity (OU, Virtual Group, Computer or User). Double-click the node to show the items contained in that node.
4. Click **Next**.
5. In the **Change Rule Actions** window, select an installation method:
   - **Install Blades Automatically** to deploy the Software Blade package automatically.
     If you select this option, continue with the next steps.
   - **Do Not Install Blades Automatically** to export the package to clients.
     Make sure that you install the correct version (32 or 64 bit) to match the client computer architecture. There are no more parameters to configure for this action. Go directly to step 8.
6. Select a **Client Version** from the list or click **Upload** to upload a different client version from in the **Packages Repository** window.
7. Click any Software Blade and then select the Software Blades to install with this rule.
   Clear Software Blades that are not to be installed with this rule.
8. Click **Next**.
9. In the **Name and Comment** window, enter a unique name for this rule and an optional comment.
10. Click **Finish** to add the rule to the **Software Deployment Rules**.
11. Click **Save**.
12. Install the policy.

### Changing Existing Deployment Rules

1. Click the **Deployment** tab and select **Software Deployment Rules**.
2. Select a rule.
3. To change the name, Double-click the **Name** cell and enter a different name.
4. To change an **Applies To** parameter, right click an entity:
   a) Select **Add new entity to this rule** and then select an entity from the tree.
   b) Select **Remove entity from this rule** to delete an entity.
5. In the **Installation Method** column, and select one of these options:
   - **Install Blades Automatically** to deploy the Software Blade package automatically.
     If you select this option, continue with the next steps.
   - **Do Not Install Blades Automatically** to export the package to clients.
     Make sure that you install the correct version (32 or 64 bit) to match the client computer architecture.
6. In the **Installed Blades** column, then select or clear Software Blades as necessary.
7. On the toolbar, click **Save**.
8. Install the policy.

### Installing Packages on Clients

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**.

### Advanced Package Settings

This section includes advanced package settings:

- Configuring VPN sites
- Uploading and removing package versions from the package repository
- Selecting a file signing method for MSI files that will be deployed using an external distribution system

### Defining a VPN Site

You can configure Endpoint Security clients to connect to a default VPN site. This is useful if your organization has an option to connect through VPNs, especially on laptops. You must include a VPN blade in the Software Blades Package to connect to the VPN site.

To **configure a client package with a default VPN site**:

1. In the **Software Deployment** tab, go to **Advanced Package Settings > VPN Client Settings**.
2. Click **New**.
3. In the **Endpoint Secure Configuration** window, enter the VPN Site details:
   - **Display Name** - Unique name for this VPN site
   - **Site address** - Site IP address or DNS name
4. 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
Deploying Endpoint Security Clients

- **SecurID KeyFob** - Endpoint users authenticate using a KeyFob hard token
- **SecurID PinPad** - Endpoint users authenticate using an SDTID token file and PIN
- **Challenge-response** - Endpoint users authenticate using an administrator supplied response string in response to the challenge prompt.

5. Click OK.

### Package Repository

Use the Package Repository to upload new client versions to the Endpoint Security Management Server.

**To upload a client package to the repository:**
1. Open the Deployment tab > Advanced Package Settings > Packages Repository.
2. Click one of these options:
   - **Upload new version MSI**
     Select a single MSI file to upload.
   - **Upload new version folder**
     Select a folder containing multiple MIS packages to upload.

**To delete a package version from the repository:**
Select an **Endpoint Version** and then click **Delete Version**.

### Configuring Software Signatures

You can make sure that endpoints in your organization receive the correct client package by adding a signature to that package. 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.

### Installing the Client Using the CLI

You can install an exported package using the CLI (run as administrator) on a client with these commands:

<table>
<thead>
<tr>
<th>Command line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msiexec /i EPS.msi /l*vd installation.log</td>
<td>Do a fresh installation of the exported package</td>
</tr>
<tr>
<td>msiexec.exe /i EPSI.msi REINSTALL=ALL REINSTALLMODE=ocmusv</td>
<td>Reinstall all installed blades using the exported package</td>
</tr>
<tr>
<td>msiexec /i EPS.msi /l*vd installation.log</td>
<td>Add an initial blade or blades</td>
</tr>
</tbody>
</table>
Deploying Endpoint Security Clients

<table>
<thead>
<tr>
<th>Command line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msiexec /i EPS.msi /l*vd installation.log /qb! REINSTALL=DUMMY REINSTALLMODE=vomus</td>
<td>Add or remove blades using the exported package</td>
</tr>
<tr>
<td>msiexec /i EPS.msi /l*vd installation.log</td>
<td>Upgrade using the specified exported package. This package must include the same blades that are presently installed.</td>
</tr>
</tbody>
</table>

**Logging Options**

To create logs, do one of the following steps:

- Add `/l*vd <path to log file>` to any of the command lines above.
- Add logging instructions to the Windows registry:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer</td>
<td>voicewarmupx</td>
</tr>
</tbody>
</table>

Windows generates the log file in the `%TEMP%` directory, and names it `MSI****.LOG`.

**Initial Security Client Analysis**

The Initial Security Client Analysis is a client that you can download to run a security analysis report on a computer. It does not require a connection to an Endpoint Security Management Server. The report shows security vulnerabilities on the computer, based on Check Point best practices.

If you connect a computer with the Initial Security Client Analysis to an Endpoint Security Management Server, it becomes a regular Endpoint Security client.

**Deploying Mac Clients**

Client packages for Mac clients must be distributed manually and do not use Software Deployment.

**To get the mac client package:**

1. In the **Deployment** tab, under **Mac Client**, click **Download**.  
   - If more than one version is in the Package repository, select a client to download.  
   - If there are no packages to select, click **Upload** and browse to the location of a Mac client package. The selected package is put in the Package Repository.

2. In the window that opens, select which blades to include in the package and click **OK**.

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.

**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 Endpoint_Security_Installer.zip to unzip the file.
   Endpoint_Security_Installer.app shows next to the zip file.
2. Click Endpoint_Security_Installer.app.
   The Check Point Endpoint Security Installer opens.
3. Click Install.
4. Enter a Name and Password to authorize the installation and click OK.
   Wait while package installs.
5. 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.

**Uninstalling the Client on Mac**

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"
   
```

   **Note** - If the endpoint was encrypted, the uninstall script first prompts for a reboot so that HFS volumes can be decrypted. After decryption, the script continues to uninstall the client.

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 32).

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

**Migrating from other Mac Products**

Migration paths are available from:
- E75 Endpoint Security VPN for Mac (and higher)
- Full Disk Encryption for Mac 3.3.5 (and higher)

Use the instructions in Upgrading Endpoint Security Clients (on page 47).
- For Full Disk Encryption, see Upgrading Legacy Full Disk Encryption (on page 50).
- If you install the Mac client on a computer that had E75 Endpoint Security VPN for Mac, it upgrades to E80.50 with its configuration settings preserved.

**Upgrading Endpoint Security Clients**

This section includes procedure for upgrading endpoint clients to E80.50.

You can upgrade to E80.50 from earlier versions of R80.x and E80.x clients with these requirements:
- You must upgrade both the Initial Client and the Software Blade Package at the same time. You cannot upgrade the Initial Client by itself.
- During the upgrade you cannot remove the Full Disk Encryption Software Blade.
- You can change all other Software Blades and all Software Blade configuration settings.

**Client Upgrade workflow:**
1. For E80.20 and earlier Endpoint Security Clients with legacy (before R80) VPN clients, remove all Firewall related blades. Do this before the upgrade.
2. Make sure that the clients are connected to an E80.50 Endpoint Security Management Server.
3. Deploy the new package to clients with one of these methods:
   - Upgrading with Deployment Rules (on page 48)
   - Upgrading with an Exported Package (on page 48)
Notes and Cautions - Windows
When upgrading to a Windows computer, be aware of these limitations:

- All packages are installed on the C drive.
- The required space on drive C is =
  Log files size (%fwdir%\log) + Conf files size (%fwdir\conf) + 4 GB
  - %fwdir%\log contains server and client logs.
  - Log file size varies for different environments.
  - %fwdir%\conf contains server configuration and client packages.
  - Client .msi files are very large.

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 Software 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 reboots the computer.

Upgrading with an Exported Package
Upgrade a client to a new package that includes the same blades as it has now. Add and remove blades after the upgraded package is installed.

To upgrade clients with an exported package:
1. In the Deployment tab, select a package and click Upgrade Profile.
   A message opens that shows if an update is available.
2. Click Yes to confirm that you want to upgrade the profile.
3. 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.
4. Click OK.
   The package EPS.msi and/or PreUpgrade.exe files are downloaded to the specified path. A different folder is automatically created for each option selected in step 3a.
5. Send the EPS.msi and 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.
**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**

See the [Release Notes](http://supportcontent.checkpoint.com/documentation_download?ID=24827) for the supported upgrade paths for this version. Legacy clients are those earlier than version R80. 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 E80.50 client with the necessary blades 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 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 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 blades 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:
Deploying Endpoint Security Clients

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 (32/64 bit) to export for laptops and desktops.
   b) Enter or browse to a destination folder.
11. Click **OK**.
The package **EPS.msi** files are downloaded to the specified path.
12. Send the **EPS.msi** 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 **EPS.msi** is installed, you can add a package with Endpoint Security Software Blades. See Upgrading with Deployment Rules (on page 48).

**Upgrading Legacy Full Disk Encryption**

See the **Release Notes** for this version for supported upgrade paths. Before you upgrade, make sure that encryption or decryption are not running.

The upgrade is done through 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.
Deploying Endpoint Security Clients

- 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 Clients ("Upgrading Endpoint Security Clients" on page 47).
- 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 Clients ("Upgrading Endpoint Security Clients" on page 47).

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 (for example, legacy FDE > E80.x > E80.50).
- 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 uninstalled the client on Windows Vista 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:
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 this solution:

<table>
<thead>
<tr>
<th>Microsoft Solution</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB311269</td>
<td>Register the WScript object by running the wscript -regserver command from a command prompt or from the Run option on the Start menu.</td>
</tr>
</tbody>
</table>

• See also DES encryption on Windows 7 clients ("Configuring Active Directory for Authentication" on page 78)

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 (on page 21) 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 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
Deploying Endpoint Security Clients

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.
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 32).

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

Configuring Log Forwarding

You can forward logs from one Endpoint Security Management Server or Policy Server to a different Endpoint Security Management Server or Policy Server.

Logs from each Endpoint Security client are reported to the Endpoint Security Server (Endpoint Policy Server or Endpoint Security Management Server) that the client is connected to.

To see all collected logs together in SmartView Tracker, you must configure Log Forwarding for each Endpoint Security Server in the SmartDashboard.

Do this procedure for each Endpoint Security Server.

**To configure Log Forwarding from one Endpoint Security Server to a different Endpoint Security Server:**

1. Open SmartDashboard and connect to the Endpoint Security Management Server.
2. Double-click the Endpoint Security Management Server object in the objects tree.
3. In the tree of the window that opens, select Logs and Masters > Log Servers.
4. In the Always Send Logs To section, Add the destination server where the logs will go.
5. Click OK.
6. Select Policy > Install Database and install the database on all hosts.
Chapter 6

Working with Endpoint Security Policies

In This Section:

Overview of Endpoint Security Policy ................................................................. 54
Software Blade Policies ....................................................................................... 55
Protection for Servers ......................................................................................... 56
Working with Rules ............................................................................................ 56
Working with Policy Actions ............................................................................... 57
Policy Toolbar ..................................................................................................... 58
Enforcing Rules According to States ................................................................. 58
Installing Policy Changes on Clients ................................................................. 59
The Heartbeat Interval ......................................................................................... 59

Overview of Endpoint Security Policy

The Endpoint Security Policy is a collection of security rules that define how Software Blades enforce security for Endpoint Security clients. Each installed and licensed Software Blade contains one or more rules.

Each Software Blade can have:

- A Default Rule (required) - Applies to all users and computers in the organization, unless there are Other Rules that match a user or computer.
- Additional Rules - One or more policy rules that apply to subgroups, users, or computers.
  - Other Rules based on Connection or Compliance state - Policy rules that are only enforced when computers included in the rule are in a specified state: Connected, Disconnected, or Restricted.

Edit the Default Rule to make it meet the needs for as much of your organization as possible. Then create Other Rules for subgroups, users, and computers that require different settings.

An Action is a collection of settings that define a specified behavior for a Software Blade. You can use the same Actions in multiple rules. Each Action that is different than the Action in the default rule shows in bold in the Policy Rule Base.

Policy rules are installed on Endpoint Security clients when you click Install.

In the Policy Rule Base:
- Right-click in a cell to:
  - Edit the cell.
  - Add a rule.
  - Remove a rule.
- Right-click an item in the Action column to change it.
# Software Blade Policies

The policy can include these Software Blades:

<table>
<thead>
<tr>
<th>Blade</th>
<th>What it does</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption</td>
<td>Combines boot protection, Pre-boot authentication, and strong encryption to ensure that only authorized users can access information stored in desktops and laptops.</td>
</tr>
<tr>
<td>OneCheck User Settings</td>
<td>Defines user-level authentication for Endpoint Security clients with Full Disk Encryption installed.</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>Protects data stored on the computers by encrypting removable media devices and allowing tight control over computers’ ports (for example, USB, Bluetooth).</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>Defines the protection of clients from known and unknown viruses and malware.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Blocks or allows network traffic based on attributes of network connections.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Makes sure that protected computers comply with your organization's security requirements. You can assign different security levels based on the compliance state. For example, non-compliance may result in a remediation message, a warning, or restriction from the network.</td>
</tr>
<tr>
<td>Application Control</td>
<td>Restricts network access on a per-application basis, allowing you to restrict network access between a particular application and the defined Access Zones.</td>
</tr>
<tr>
<td>Client Settings</td>
<td>Defines a common policy that affects multiple blades. The settings include: Installation settings, branding, logging and some settings for Network Protection blades.</td>
</tr>
<tr>
<td>Access Zones</td>
<td>Defines the topology of the organizational network, separating it into Trusted and Internet domains.</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>Detects bot-infected machines and blocks bot C&amp;C communication for users on the organizational network and outside of the organizational network.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Lets organizations control access to web sites by category, user or group, and this way improves network security and enhances user productivity.</td>
</tr>
<tr>
<td>Secure Mobile Documents</td>
<td>Lets organizations protect and share documents safely with internal and external users, and also manage, monitor, and deploy the organizational Check Point Document Security policy through SmartEndpoint.</td>
</tr>
<tr>
<td>Forensics</td>
<td>Monitors files and the registry for suspicious processes and network activity. When the Anti-Malware or the Anti-Bot Client Software Blade, or the Check Point Gateway Software Blade detects an attack, the Check Point Endpoint Forensics Software Blade analyzes the attack, and uploads the complete attack report to the Endpoint Security Management Server.</td>
</tr>
</tbody>
</table>

Settings for some Software Blades are defined for computers, while others are defined for users.

For example:

- The Firewall policy applies to users, and is enforced for users on all company computers they log on to.
- The Full Disk Encryption policy applies to the computer. For all users that log on to a computer, the disk encryption policy stays the same.
Protection for Servers

These blades 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 Windows Server.

To disable Application Control on servers:

a) Assign the server group or members to a new application control policy.
b) Disable application control in the policy.
c) Install the policy.

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 ("Types of Virtual Group" on page 37).


Working with Rules

A rule is a set of predefined actions that a Software Blade does to enforce security on specified users and computers. Each Software Blade has one default rule that applies to all endpoint computers and users that are not assigned to a different rule. You can change the default rule settings, but you cannot delete it.

Each rule contains one or more:

- Scope definitions that assign the rule to specified users and computers (on page 28).
- Action definitions ("Working with Policy Actions" on page 57) that define the Software Blade behavior when enforcing security.

Inheritance and Rule Priority

The default rule, located at the top of each blade section, applies to all users and computers that are not protected by a different rule. User-defined rules show below the default rule.

Endpoint Security assigns the matching first rule (after the default rule) for each blade.

The first Other Rule that a user or computer matches for each blade is applied. If no Other Rule matches, the default rule applies.

For example, user Jane Collins is in the Human Resources department and uses a laptop.

- In the rules for Full Disk Encryption, a rule for All Laptops is the first rule that Jane matches. Its settings are applied.
- In the rules for Firewall, a rule for Human Resources is the first rule that Jane matches. Its settings are applied.
- In the rules for Anti-Malware, there are no Other Rules that match Jane. The Default Rule applies.

Make sure that rules for specified users or computers are located above those for groups and containers they are members of. For example:

- If you require a rule for the company CEO, make sure to put that rule above rules for groups that the CEO belongs to.
- If you create rules for servers, make sure the rules are above all other rules that might include servers as part of a group or Network.
Creating New Policy Rules

Each Software Blade has a default rule in the Policy Rule Base. The default rule applies to the Entire Organization unless there are Other Rules that match a user or computer.

If you create more rules for a blade, the first rule that a user or computer matches in the Other Rules section is applied.

To create a new policy rule:
1. Right-click in a policy rule to create a new rule for the same blade. The Create Rule Wizard opens.
2. On the Select Enforcement state page, select Add Rule for and select a state:
   • When Connected
   • When Disconnected (only shows when applicable for that blade)
   • When Restricted (only shows when applicable for that blade)
3. On the Select Entities page, select those OUs, groups or individuals that this rule applies to.
4. On the Change Policy Actions, right-click the applicable actions and configure as necessary.
5. On the Finish page, Enter a descriptive Name and optionally Comments.
6. Click Finish.
7. Click Install to install the policy on Endpoint Security clients.

Working with Policy Actions

An Action is a collection of settings that define a specified behavior for a Software Blade.

For each Action, you can:

- Right-click and select one of the predefined options.
- Right-click and select Edit or double-click to open the Properties of the Action. You can see the predefined settings and change them as necessary.
- Right-click and select Create Custom to configure all settings for that Action.
- After you create a changed or custom Action, you can select that Action to use it again in other rules.
- In the Select action field of the Action Properties, select New to rename an Action. You can rename an Action to show changes that you made and make it easier to use the Action again in other rules.

If you change the properties of a predefined or New Action, those properties become part of the Action. If you select that Action again in a different rule, it will include the changed properties.

For example, in the Properties of the Anti-Malware Action, Perform periodic anti-malware scan every month, you change the Day of month that the scan occurs to 2:

- For each rule that contains that Action, the scan occurs on Day 2 of the month.
- If you change the Day of month value to 3 in one rule where the Action is used, it will change in all rules that contain that Action.

Each Action that is different than the Action in the default rule shows in bold in the Policy Rule Base.

If an Action shows the Wide Impact icon, the Action is the same in all rules.
**Policy Toolbar**

These options are available from the toolbar of the Policy:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Create Rule]</td>
<td>Create a policy rule for the selected blade that applies to a subgroup or individual. By default the policy you create applies when users are connected to an Endpoint Security server. To create a policy that applies when users are in a different state, click the downward arrow and select a state from the list. Only states that are applicable for a blade show as options.</td>
</tr>
<tr>
<td>![When Connected]</td>
<td>Create a policy rule that applies when users are connected to an Endpoint Security server. This rule also applies if there is no applicable rule for the Disconnected or Restricted states.</td>
</tr>
<tr>
<td>![When Disconnected]</td>
<td>Create a policy rule that applies when users are NOT connected to an Endpoint Security server.</td>
</tr>
<tr>
<td>![When Restricted]</td>
<td>Create a policy rule that applies when a computer's compliance state is Restricted. This occurs when a computer is not in compliance with the enterprise security requirements.</td>
</tr>
<tr>
<td>![Delete Rule]</td>
<td>Delete the selected policy rule.</td>
</tr>
<tr>
<td>![Save]</td>
<td>Save all changes to the Policy.</td>
</tr>
<tr>
<td>![Refresh]</td>
<td>Refresh the page to show the most updated information.</td>
</tr>
<tr>
<td>![Install]</td>
<td>Install the policy on Endpoint Security clients.</td>
</tr>
<tr>
<td>![Highlight text]</td>
<td>Enter text to search for a word or text string in the Policy Rule Base. The text that matches is highlighted in the Rule Base.</td>
</tr>
<tr>
<td>![Show Policy for]</td>
<td>Filter the Rule Base to only show the policies that apply for a specified group, user, or computer. Use the arrow or ... button to select a node. Click <strong>Clear</strong> to show the full Rule Base.</td>
</tr>
</tbody>
</table>
| ![Show or hide Actions that are different than the default rule] | Toggle between two settings to define which actions show in the Rule Base:  
- Hide Actions that are included in the Entire Organization policy rule to only show Actions that are specific to Other Rules.  
- Show all Actions included in the policy. Actions that are different than the Entire Organization policy show in bold. |
| ![Move rules up or down] | Click the arrows to change the sequence of a selected policy rule in the **Other Rules** for a Software Blade. The sequence defines the priority of the rules.  
You can also change the sequence of the rules by dragging and dropping rules in the Rule Base. |

**Enforcing Rules According to States**

Endpoint Security can enforce policy rules on computers and users based on their connection and compliance state. When you create a policy rule, you can select the state or states during which this policy is enforced. By default, policies apply when the client is **Connected**.
States are not applicable for all blades. For example, Full Disk Encryption rules always apply and cannot change based on state. The option to create rules based on state only shows for applicable blades. If there is no applicable rule for the Disconnected or Restricted states, the **Connected** policy applies.

- The **Connected** state policy is enforced when a compliant endpoint computer connects to the Endpoint Security Management Server.
- The **Disconnected** state policy 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.
- The **Restricted** state policy is enforced when an endpoint computer is not in compliance with the enterprise security requirements. Its compliance state is moved to **Restricted**.
  
  In the Restricted state, you usually choose to prevent users from accessing some, if not all, network resources.

You can configure restricted state policies for these blades:

- Media Encryption & Port Protection
- Firewall
- Access Zones
- Application Control

### Installing Policy Changes on Clients

When you save the Policy, Endpoint Security does not automatically deploy it. This behavior lets you save changes to the Policy without affecting users. It also lets you deploy the Policy at the most convenient time, for example, at night.

**To install the Policy on Endpoint Security clients:**

- In the Policy tab, click **Install**.
- or
- From the **File** menu, select **Install Policies**.

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

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.

### The Heartbeat Interval

Endpoint computers send “heartbeat” messages to the Endpoint Security Management Server to make sure that all connections are active and that all policies are up to date. The time between heartbeat messages is known as the **heartbeat interval**.

**Note** - The default heartbeat interval is 60 seconds.

A heartbeat interval that is too short can cause performance degradation. A heartbeat interval that is too long can cause security degradation and less accurate reporting.

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.

**To configure the heartbeat interval:**

1. Click **Manage > General Properties**.
   
   The **General Properties** window opens.
2. In the **Connection Settings** section, set the **Interval between client heartbeats**.
3. 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. In the Endpoint Security console, select **Manage > General Properties > Connection Settings**.
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:
\[ \text{<number of heartbeats>} \times \text{<heartbeat interval (in seconds)> } \times 60.\]
Chapter 7

External Endpoint Policy Servers

In This Section:

- Overview of Endpoint Policy Servers ................................................................. 61
- Installing and Configuring an Endpoint Policy Server ............................................. 61
- How do Endpoint Policy Servers Work? ................................................................. 62
- Configuring Policy Server Settings ......................................................................... 63
- Monitoring Endpoint Policy Server Activity ............................................................. 65

Overview of 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.

To install an Endpoint Policy Server:


Configuration on R77 and R77.10 Management

⚠️ Important - When you add an Endpoint Policy Server to a High Availability deployment, you must install the database in SmartDashboard on all Endpoint Security Management Servers and the Endpoint Policy Server. To do this, select Policy > Install Database.

To create an Endpoint Policy Server object and establish SIC trust:

1. Log in to SmartEndpoint using the IP address and credentials for the Primary Endpoint Security Management Server.
2. Select Manage > General Properties.
3. In the Endpoint Policy Servers pane, click New.
4. In the Select New Object Type window, select Host and click OK. The Host Properties window for the server opens.
5. Enter a Name for the Endpoint Policy Server and its IP address.
6. Click Communication to create SIC communication with the Endpoint Security Management Server.
7. In the **Communication** window:
   a) Enter and confirm the **SIC Activation Key** that you gave the Policy Server.
   b) Click **Initialize** to create a state of trust between the Endpoint Policy Server and the Endpoint Security Management Server.
   c) If the trust is not created, click **Test SIC Status** to see what you must do to create the trust successfully.
   d) If you have to reset the SIC, click **Reset** to reset the SIC and then click **Initialize**.
   e) Click **Close**.

8. Click **OK**.

9. Select **File > Install Policy**.

**To complete the Endpoint Policy Server configuration:**
1. In SmartEndpoint, select **Manage > General Properties**.
3. In the object properties window, click **Install Database**. This establishes communication with the Endpoint Policy Server.
4. After the installation process completes click **Close** in the **Install Database** window.
5. Click **OK**.
6. If a High Availability Secondary server exists, perform step 1-4 on the Secondary server object also.
7. Open the Endpoint Policy Server object (created in the "Create an Endpoint Policy Server object" procedure).
8. In the object properties window, click **Install Database**.
   This step establishes communication with the Endpoint Security Management Server and lets the Endpoint Policy Server collect logs.
9. After the installation process completes, click **Close** in the **Install Database** window.
10. Click **OK**.
11. Click **OK**.
12. Click **Save**.
13. If you see an **Enforce Changes** message that prompts you to save the changes, click **Save & Install**.
14. If you did not click **Save & Install**, select **File > Install Policies**.
   The Endpoint Policy Server synchronizes with the Endpoint Security Management Server after the policy and databases are installed. This can take a while, based on the quantity of policies and installation packages.

**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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active Directory Domains</td>
</tr>
<tr>
<td>2</td>
<td>Endpoint Security Management Server</td>
</tr>
<tr>
<td>3</td>
<td>External Endpoint Policy Server</td>
</tr>
<tr>
<td>4</td>
<td>Enterprise workstations with Endpoint Security clients installed</td>
</tr>
</tbody>
</table>

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
- 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 blade-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 > General Properties > Connection Settings**.
2. Enter or select the **Interval between client heartbeats** ("The Heartbeat Interval" on page 59) value (Default = 60 seconds).
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** ("Configuring the "About to be Restricted" State." on page 60) value (default = 5 heartbeats).
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 > General Properties > 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.

**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 SmartDashboard.
- **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.
Chapter 8

Management High Availability

In This Section:

- Overview of Management High Availability ............................................................. 67
- Configuring a Secondary Server in SmartDashboard ............................................. 68
- Failover ................................................................................................................... 69
- Synchronizing Active and Standby Servers ............................................................ 70
- Environments with Endpoint Security ..................................................................... 73
- Disaster Recovery with High Availability ................................................................. 75

Overview of Management High Availability

Security Management High Availability lets you create one or more synchronized management servers for redundancy and database backup. If 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.

The Security Management Server contains multiple databases for both Network Security and Endpoint Security. These databases contain policies, rules, user definitions, endpoint deployment packages, network objects, and system configuration settings. It is important to back up this data, so that crucial information is not permanently lost in the event of a server failure.

In addition, if the Security Management Server fails or is off line for maintenance, a backup server is available to take over its activities.

The High Availability Environment

A Management High Availability environment includes:

- One Active Security Management Server
- One or more Standby Security Management Servers

Active server databases are periodically synchronized with the Standby server databases for full redundancy.

Active vs. Standby

Only the Active server manages gateways, network objects, system configuration, and endpoint clients. Only one Security Management Server can be Active at a time. If the Active server fails, you manually change a Standby server to the Active server. You can change an Active server to Standby and a Standby to Active at any time.

You can use SmartConsole applications on the Secondary server in Read Only mode.

Primary Server vs. Secondary Server

When you install your first Security Management Server, you define it as the Primary Security Management Server. Typically this becomes the initial Active Security Management Server. When you install more Security Management Servers, you must define them as Secondary Security Management Servers. When ready for use, the Primary and Secondary servers can work as Active or Standby Security Management Servers as necessary.
A Secondary Security Management Server is ready for use when these steps are completed:

- It is defined in SmartDashboard as a network object.
- SIC trust is established with the Primary Security Management Server.
- It is synchronized with the Primary Security Management Server for the first time. You must do this manually.

**Planning for Management High Availability**

When you plan your High Availability deployment, think about these issues:

- **Remote versus Local Installation of the Standby Security Management Server** - It is good to install a Standby Security Management Server remotely and not on the LAN. If there are connectivity issues on the LAN the remote Standby Security Management Server will not be affected.
- **Different physical locations** - It is good to have at least one Standby Security Management Server in a different location than the Active Security Management Server to have High Availability in a disaster situation.
- **Data overload during synchronization** - The data saved during synchronization is very heavy. Synchronization is optimized if the connectivity between the Security Management Servers is quick and efficient.

**Configuring a Secondary Server in SmartDashboard**

In the SmartDashboard connected to the Primary server, you create a network object to represent the Secondary Security Management Server. You then synchronize the Primary and Secondary Security Management Servers.

**To configure the secondary server in SmartDashboard:**

1. Open SmartDashboard.
2. In the **Network Objects** tree, right-click **Check Point** and select **Host**.
3. In the **Check Point Host** window, enter a unique name and IP address for the server.
4. In the **Software Blades** section, select the **Management** tab.
5. Select **Network Policy Management**. This automatically selects the **Secondary Server, Logging and Status**, and **Provisioning** options.
6. Optional: To use Endpoint Security, select **Endpoint Policy Management**.
7. Click **Communication** to create SIC trust between the Secondary Security Management Server and the Primary Security Management Server.
   a) Enter and confirm the SIC Activation Key that you entered in the Check Point Configuration Tool.
   b) Click **Initialize** to create a state of trust between the Security Management Servers.
   c) If the trust is not created, click **Test SIC Status** to see what you must do to create the trust successfully.
   d) If you have to reset the SIC, click **Reset**, reset the SIC on the Secondary Server and then click **Initialize**.
   e) Click **Close**.
8. Click **OK**.
9. Select **File > Save**.

For environments with Endpoint Security, see Manual Synchronization with Endpoint Security (on page 73).
Failover

Security Management Server failover is a manual procedure. If the Active Security Management Server fails or it is necessary to change the Active Security Management Server to a Standby, you must do these steps to prevent data loss:

If the Active Security Management Server is responsive:
1. Manually synchronize the Active and Standby Security Management Servers.
2. Change the Active Security Management Server to Standby ("Changing a Server to Active or Standby" on page 69).
3. Change the Standby Security Management Server to Active ("Changing a Server to Active or Standby" on page 69).

If the Active Security Management Server has failed and you cannot change it:
Manually change the Standby Security Management Server to Active ("Changing a Server to Active or Standby" on page 69).

Important: If you have two Security Management Servers that are set to Active at the same time, unexpected behavior can occur.

If your environment includes Endpoint Security:
After you change the Standby Security Management Server to Active, edit the PAT version on the new Active Security Management Server ("Updating the PAT Version on the Server" on page 74).

Changing a Server to Active or Standby

Whenever possible, change the Active Security Management Server to Standby before you change the Standby Security Management Server to Active.

To change an Active Endpoint Security Management Server to Standby:
1. Connect to the Active Security Management Server with SmartDashboard.
2. Go to Policy > Management High Availability.
3. Click Change to Standby.
4. Click Yes to confirm the change.

To change a Standby Security Management Server to Active:
1. Connect to the Standby Security Management Server with SmartDashboard.
2. The Server Login window opens.
3. Make sure that no peer server is Active.
4. Click Change to Active.
5. Click Yes to confirm the change.

Understanding Server Status

Before you make changes to the High Availability environment, make sure that you know the status of each Security Management Server. It is very important to know which Security Management Servers are in Active mode and which are in Standby.

To see the status of the servers in your High Availability environment:
1. In the SmartDashboard of a Security Management Server, select Policy > Management High Availability.
2. In the localhost window that opens, see the status of the Security Management Server you are on in My Status.
3. See the status of other Security Management Servers in Peer Status.

The fields are:
### Field | Values | Description
--- | --- | ---
Server Name | Any | The SmartDashboard name of the server.
Type | Primary or Secondary | This is only the order of the installation and does not impact the environment.
Mode | Active or Standby | If the Security Management Server is currently Active or Standby.
Reachable | Yes or No | This field is only in the Peer Status. It shows if the local server has connectivity with that peer.
Status | Never been synchronized, Synchronized, Lagging, Database has been changed, Advanced, or Collision | The status of synchronization between the Security Management Servers. See Synchronization Status (on page 72) for complete descriptions.

#### Synchronizing Active and Standby Servers
After you install the Standby servers, you must do the first synchronization manually even if you configure the system for automatic synchronization. After the first synchronization, you can configure the frequency of automatic synchronization.

#### Synchronization Procedures

**Note** - While the synchronization is in progress, the databases are locked. A message shows in SmartEndpoint. SmartDashboard shows a Not Responding message.

**To synchronize manually:**
1. In SmartDashboard connected to the Primary or Secondary server, select File > Policy > Management High Availability.
2. Click Synchronize.
3. Click OK.

**To configure when Synchronization occurs:**
1. In SmartDashboard, go to Policy > Global Properties > Management High Availability.
2. Select from the options:
   - **Automatic Synchronization when policy is installed** - If you choose to have the synchronization occur automatically, the Active and Standby Security Management Servers automatically synchronize each time the Policy is installed in SmartDashboard or SmartEndpoint.
     
     You can choose to do automatic synchronization more frequently. If you choose one of these options, the synchronization also starts when the Security Policy is installed:
     
     - **Every time a policy is saved** - Synchronizes each time a policy is saved in SmartDashboard or SmartEndpoint.
     - **On scheduled event** - Synchronizes based on a schedule that you set, for example, daily at 1:00 AM, or every three hours.
     
     **Important** - If you set the synchronization to occur at regular time intervals, do not set it to be more frequent than every 1 hour.
   - **Manual synchronization only** - If you select this, you must start a manual synchronization each time it is necessary to synchronize the Active and Standby Endpoint Security Management Servers.
3. Optional: For Type of notification for Management High Availability tracking, select the way you are notified about changes in the High Availability environment. The default is through Popup Alerts.
4. Click OK.

If automatic synchronization is selected as the synchronization mode, you can also synchronize manually when necessary.

**Which Data is Synchronized**

When synchronization occurs, this data is backed up and synchronized:

- **Network Security Management Server databases:**
  - Network security polices and settings
  - Network objects
  - Services and resources
  - Check Point User Database
  - OPSEC applications
  - Custom queries and reports

- **Configuration and Internal Certificate Authority data:**
  - Databases (such as the Objects and Users).
  - Certificate information such as Certificate Authority data and the CRL which is available to be fetched by the Check Point Security Gateways.

- **The Endpoint Security databases:**
  - Objects: Computers, users and Servers (including Active Directory data)
  - Client deployment rules
  - Custom reports

![Important - Endpoint Security client deployment packages (MSI files) and Smart Card drivers are NOT synchronized. In an environment with Endpoint Security, you must manually copy these items to the Standby servers.]

**How Synchronization Works**

Synchronization can run automatically or you can start it manually. When synchronizing, the system does these steps without user intervention:

1. Locks the policy and object databases on the Active Security Management Server.
2. Takes a snapshot of the databases and save it to local disk.
3. Unlocks policy and object databases.
5. The Standby Security Management Servers overwrite their databases with the snapshot.
7. The Active and Standby servers delete the snapshots.

While the Active Security Management Server is taking a snapshot (step 2 above), the databases are locked and you cannot add, change or delete these system objects:

- Security Gateways, Security Management Servers and other network objects
- VPN Communities
- Services, resources and OPSEC applications
- Policies and rules
- Deployment rules and packages
- Reports and queries
This is necessary to prevent database corruption and other errors.

If the environment includes Endpoint Security, the Active Security Management Server and clients continue
to dynamically update these database objects even while the Security Management Server takes a
snapshot:

- Full Disk Encryption recovery data
- Media Encryption & Port Protection recovery data
- Endpoint monitoring data
- Endpoint heartbeat data

**Synchronization Status**

The synchronization status shows the status of the peer Security Management Servers in relation to the
selected Security Management Server. You can see this status if you are connected to the Active Security
Management Server or a Standby Security Management Server. The Synchronization Status is in the
SmartDashboard > **Management High Availability Servers** window in the **status** column or in SmartView
Monitor.

The possible synchronization statuses are:

- **Never been synchronized** - A newly installed Secondary Security Management Server has not yet
  been manually synchronized with the Active Security Management Server.
- **Synchronized** - The Secondary Security Management Server is fully synchronized with the Active
  Security Management Server. The databases are identical.
- **Lagging** or **Database has been changed** - Changes were made to the Active Security Management
  Server after the last synchronization, which were not synchronized with the Standby Security
  Management Servers. This can occur when changes are made to the Active Security Management
  Server database during the Synchronization process.
- **Advanced** - The Standby Security Management Server is more up-to-date than the Active Security
  Management Server. This can occur after there was a failover to the Standby and then a second failover
  back to the original Active server.
- **Collision** - The Active Security Management Server and Standby servers have different policies and
databases and it is not immediately obvious which server is the most up-to-date. This can happen when
an Active server fails over to a Standby and the Standby fails over back to the Active server before
synchronization.

  In this case, make a decision as to which Security Management Server contains the most recent
  updates. Usually this is the Security Management Server that has more changes. If necessary, change
  this Security Management Server status to Active and all others to Standby.

  Manually synchronize the newly specified Active Security Management Server to the Standby servers.
  For Endpoint Security, it might also be necessary to update the PAT version on the Security
  Management Server.

You can use SmartView Tracker to monitor management and synchronization operations.

**Synchronization Troubleshooting**

The synchronization can fail in these situations:

- Failure for technical reasons, for example the Active Security Management Server did not connect with
  the Standby Security Management Server. To resolve this you can do one of these when the technical
  problem is fixed:
  - Manually synchronize the Standby Security Management Server.
  - If automatic synchronization is configured, install the Policy again on the Active Security
    Management Server. Then synchronization occurs automatically.

- A collision occurs between the Security Management Servers. In this situation the system administrator
does a manual synchronization and chooses which database is the dominant database. The CA is
  always merged to prevent security issues.
Management High Availability

When a collision occurs and one of the Security Management Servers is overwritten, you can use the Audit Logs in SmartView Tracker to better understand the situation. We recommend that you look at the management operations done recently on the overwritten Security Management Server. Do these operations again, if necessary, on the dominant Security Management Server.

Environments with Endpoint Security

Environments that include Endpoint Security require some additional steps for:

- The initial manual synchronization
- Failover
- Synchronization of MSI files and drivers

**Important** - When you add an Endpoint Policy Server to a High Availability deployment, you must install the database in SmartDashboard on all Endpoint Security Management Servers and the Endpoint Policy Server. To do this, select Policy > Install Database.

Manual Synchronization with Endpoint Security

To synchronize Security Management Servers with Endpoint Security manually:

1. In SmartDashboard of the Active Security Management Server, select Policy > Management High Availability.
2. Click Synchronize.
3. Click OK.
4. Select Policy > Install database
5. In the first synchronization after installation, the Servers automatically synchronize again according to the settings configured in SmartDashboard, including the synchronization schedule. If you configured the manual synchronization settings in SmartDashboard, you must synchronize manually.
   While the synchronization takes place, SmartDashboard shows Not Responding.
6. Do the steps in Synchronizing MSI Files and Drivers (on page 73).

Synchronizing MSI Files and Drivers

Each time you download a new MSI package or driver that is related to Endpoint Security, for example, a Smart Card driver, you must synchronize these files throughout the High Availability environment. This is not done automatically with synchronization because the files can be very large.

To synchronize MSI 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:
      - On Windows platforms: %fwdir%\conf\SMC_Files\uepm\msi
      - On SecurePlatform or Gaia: $FWDIR/conf/SMC_Files/uepm/msi
   
   b) On the Standby Security Management Server, replace these folders with the folders that you copied from the Active Security Management Server:
      - On Windows platforms: %fwdir%\conf\SMC_Files\uepm\msi
      - On SecurePlatform or Gaia: $FWDIR/conf/SMC_Files/uepm/msi

   c) If necessary, manually copy the Smart Card drivers.
      - On Windows platforms: %fwdir%\conf\SMC_Files\uepm\DRIVERS
      - On SecurePlatform or Gaia: $FWDIR/conf/SMC_Files/uepm/DRIVERS

d) On Gaia, SecurePlatform or Linux computers, run:
   
   (i) cd $FWDIR/conf/SMC_Files/uepm
2. On the Standby Security Management Server, replace these folders with the folders that you copied from the Active Security Management Server:
   - On Windows platforms: %fwdir%\conf\SMC_Files\uepm\DRIVERS
   - On SecurePlatform or Gaia: $FWDIR/conf/SMC_Files/uepm/DRIVERS

### 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 you cannot synchronize the Security Management Servers before you change a Standby server to Active, this will probably occur. 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:
   - **Windows:** `uepm patver set <old_PAT_version_number> + 10`
   - **SecurePlatform and Gaia:** `uepm patver set <old_PAT_version_number> + 10`
3. Make sure the new PAT version is set by running:
   - **Windows:** `uepm patver get`
   - **SecurePlatform and Gaia:** `uepm patver get`

### Synchronization with Endpoint Security

Network Security Management Servers (without Endpoint Security) only synchronize static configuration data. These Active and Standby servers stay synchronized until policies or other objects are changed.

When the High Availability environment includes Endpoint Security, some Endpoint Security data is updated dynamically, even while synchronization occurs. Dynamic updates are necessary to make sure that critical communication between the Active Security Management Server and clients is always available. For example, recovery data for Full Disk Encryption and Media Encryption & Port Protection, endpoint monitoring data, and endpoint heartbeat data is dynamically updated during synchronization.

Dynamic updates during synchronization can cause Active and Standby Security Management Servers to be out of synchronization (in the Lagging status) almost immediately after the synchronization completes. This behavior is normal for Security Management Servers with Endpoint Security.
Disaster Recovery with High Availability

In a situation where the Primary server becomes permanently unavailable, you must promote the Secondary server to Primary or create a new Primary server. By default, the first server installed is called the Primary server. You can only export the database from a Primary server. It is not sufficient to do the failover procedure and change the Standby server to Active.


In addition, licenses are linked to IP addresses. At the end of the disaster recovery you must make sure that licenses are correctly assigned to your servers.

Choose from one of these workflows:

- Create a new Primary server with the IP address of the original Primary server ("Recovery with a New Primary Server" on page 75) (not supported for environments with Endpoint Security).

- Promote the Secondary server to Primary and create new licenses.

Recovery with a New Primary Server

Note - This procedure is not supported for environments with an Endpoint Security Management Server. Use Recovery by Promoting a Secondary Server in environments with Endpoint Security.

After your Primary server becomes permanently unavailable:

1. Change the Secondary server from Standby to Active.
2. Install a new Primary server with the same IP address and hostname as the original Primary server.
3. Synchronize the new Primary server with your Active server.
4. Change the new Primary server to the Active server and the original Secondary server to Standby.
5. Promote the new Primary server to be Primary ("Promoting a Secondary Server to Primary" on page 75).
6. Make sure the licenses work and if necessary, reassign them.

Recovery by Promoting a Secondary Server

After your Primary server becomes permanently unavailable:

1. Promote the Secondary server to Primary ("Promoting a Secondary Server to Primary" on page 75).
2. Create and install new licenses.
3. Delete the original Primary server from the database.
4. Install a new Secondary server and synchronize it with the Primary server.

Promoting a Secondary Server to Primary

The first management server installed is the Primary Server and all servers installed afterwards are Secondary servers. As part of disaster recovery with High Availability it might be necessary to promote a Secondary server to become the Primary server.

Before you start, synchronize two Secondary servers. It might be necessary to create a new Secondary server to do this.

To promote a Secondary server to become the Primary server:

1. On the Secondary Server that you will promote, run cpstop to stop all Check Point services.
2. Edit the objects_5_0.c file:
   a) Edit the Primary Object definitions to look like this:

```cpp
:primary_management (true) @ :primary management (false)
Remove from admin_info the following attribute :Deleteable (false)
```
b) Edit the Secondary Object Definitions to look like this:

```
:primary_management (false) © :primary management (true)
Add under admin_info the following attribute :Deleteable (false)
```

3. To change the registry and set this server to be the Primary server, run: cpprod_util FwSetPrimary 1

4. Remove the $FWDIR/conf/mgha* files. They contain information about the current Secondary settings. These files will be recreated when you start the Check Point services.

5. Make sure you have a mgmta license on the newly promoted server.

6. Run cpstart on the promoted server.

7. In SmartDashboard:
   a) Remove all instances of the old Primary Management object. Right-click the object and select Where Used to see all of the instances.
   b) Delete the old Primary Management object.

8. In SmartDashboard, in the new Primary server object, go to Gateway Properties > Logs. Make sure logs that were sent to the old server are sent to the new Primary server.

9. Synchronize Secondary servers with the Primary server.
Chapter 9

Endpoint Security Active Directory Authentication

In This Section:

- Configuring Authentication ................................................................. 78
- Configuring Active Directory for Authentication ................................. 78
- Configuring Global Authentication ...................................................... 79
- Troubleshooting Authentication in Server Logs ..................................... 80
- Troubleshooting Authentication in Client Logs ...................................... 81

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 system can function in different modes:

- **Unauthenticated** mode - Connecting computers and users working on them are not authenticated. They are trusted "by name". This operation mode is recommended for evaluation purposes only. While in Unauthenticated mode, the SmartEndpoint will show **Unauthenticated Mode** in its Status bar (at the bottom of the Console window).

- **Strong Authentication** mode - Each connecting computer and the user working on it are authenticated with the Endpoint Security Management Server, using industry-standard Kerberos protection through the Active Directory server.
  This option is only available for endpoints that are part of Active Directory.

The authentication process:

1. The Endpoint Security client (2) requests an authentication ticket (1) from the Active Directory server (3).
2. The Active Directory server sends the ticket to the client.
3. The client sends the ticket to the Endpoint Security Management Server.

The default behavior after Security Management Server installation is **Unauthenticated** mode. It is recommended that you use this mode while you are evaluating Endpoint Security, in a lab environment; and that you change to **Strong Authentication** 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, Full Disk Encryption and Media Encryption & Port Protection are only supported on endpoint computers that are part of Active Directory.

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 Authentication

When you are ready to move to production and to set up Strong Authentication follow this process. Do not set up authentication before you are ready to move to production, and do not leave your production environment without authentication.

**To efficiently move to Strong Authentication:**

1. Configure the Active Directory for authentication.
2. Configure the Authentication Settings.
3. Install Policies.
   - The server communicates to clients that they now work in Authenticated mode.

### Configuring Active Directory for Authentication

Endpoint Security Strong Authentication uses the Kerberos network authentication protocol. To configure this service, run `ktpass.exe`.

- In Windows Server 2008, `ktpass` is included by default.

⚠ **Important** - In the procedure below you create a user that is mapped to the ktpass service. After you create this user, do not make changes to it, for example, do not change the password. If you do change the user, the key version increases and you must update the **Key version number** in the **Active Directory SSO Configuration** window in the SmartEndpoint.

**To prepare the Active Directory Server for authentication:**

1. Run `ktpass.exe`.
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
Where:
ServiceName= tst
realm (domain name)= NAC1.COM (in princ command: the first time in lower case and the second in upper case)
userName = auth-user (user from item 4)
userPass = 123456 (password for user from item 4)
name of outFile = outfile.keytab = 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 (0x32ed87bd5f0c5e9c8a8547376818d4)

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 (http://supportcontent.checkpoint.com/solutions?id=sk64300).

Configuring Global Authentication

You can configure the Authentication Settings for deployment packages.

Important - Use the Unauthenticated mode only for evaluation purposes. Never use this mode for production environments. Configure the authentication settings before moving to production.

To configure authentication settings:
1. In SmartEndpoint open Manage > General Properties > Authentication Settings.
2. Click Add.
The Active Directory SSO Configuration window opens.
3. Enter the details of the configured Active Directory, taken from the output of ktpass, the Active Directory map service command ("Configuring Active Directory for Authentication" on page 78).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name</td>
<td>Active Directory domain name</td>
</tr>
<tr>
<td>Principle Name</td>
<td>Authentication service name in the format: SERVICE/realm@REALM</td>
</tr>
<tr>
<td></td>
<td>This value must match what was done in Active Directory &gt; New Object.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter (and confirm) the password of the Active Directory Domain Admin user you created for Endpoint Security use.</td>
</tr>
<tr>
<td>Ticket encryption method</td>
<td>Select the encryption method according to the Active Directory output.</td>
</tr>
<tr>
<td>Key version number</td>
<td>Enter the version number according to the Active Directory output.</td>
</tr>
</tbody>
</table>

4. Click OK.
5. When you are ready to work in Authentication mode, select Work in authenticated mode in the Authentication Settings pane.
When you configure client package profiles, you will have to choose an authentication account. The SSO Configuration details will be included in the client package, allowing the server to authenticate the client.

**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 ("Directory Synchronization" on page 34).

**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 %uepmdir%\logs\Authentication.log.

**To see full debugging information in the Authentication.log file on a Windows server:**

1. On the Endpoint Security server, right-click **My Computer** and select **Properties**.
2. In the **Advanced** tab, click **Environment Variables**.
3. Select the variable **TDERROR_ALL_KERBEROS_SERVER** and click **Edit**.
   - If this variable does not exist, create it.
4. Change the value of the variable to 5.
5. Click **OK**.
6. Click **OK**.
7. Restart the Endpoint Security server.

**To see full debugging information in the Authentication.log file on a Gaia server:**

2. Restart the Endpoint Security server.

**Results in Authentication.log**

- If the **Authentication.log** file on the server shows:
  
  The database was cleaned or the process to include authentication in the client package was faulty. To fix:
  
  a) Repeat the process to configure authentication ("Configuring Authentication" on page 78).
  
  b) Make a new client package.
  
  c) Restart the Endpoint Security server.

- If the **Authentication.log** file on the server shows:
  
  Restart the Endpoint Security server.

- 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 %UEPMDIR%\engine\conf\global.properties, 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 ("Configuring Active Directory for Authentication" on page 78).

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 in the Check Point Endpoint Security Management.
Chapter 10

Backup and Restore

Overview of 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.

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

To Back up Endpoint Security data:
1. Open a command prompt on the source server.
2. Change directory to: %FWDIR%\bin\upgrade_tools
3. Run migrate.exe export with the full path to the output (.tgz) file.

For example: %FWDIR%\bin\upgrade_tools> migrate.exe export <output_file_name>

The <output_file_name> can be the output file path. If you do not include an output file path, the utility generates the tgz file in the %FWDIR%\bin\upgrade_tools directory.
To restore Endpoint Security data:
1. Copy the .tgz file from the source server to the target server.
2. Open a command prompt.
3. Change directory to: %FWDIR%\bin\upgrade_tools
4. Run migrate.exe import with the full path to the input (.tgz) file.
   For example: %FWDIR%\bin\upgrade_tools> migrate.exe import <input_file_name>
   The migrate utility:
   • Extracts the configuration files from the .tgz.
   • Copies them to the correct places.
   • Restores the Endpoint Security management and Security Management Server databases.
5. When prompted, restart the target server.

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.

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:
   • Windows - %uepmdir%\bin>
   • SecurePlatform and Gaia - $UEPMDIR/bin
3. Run the Endpoint Security Management Security utility (uepm.exe) and set the new PAT version:
   Windows: %uepmdir%\bin>uepm patver set <old_PAT_version_number> + 10
   SecurePlatform and Gaia: $UEPMDIR/bin>uepm patver set <old_PAT_version_number> + 10
4. Make sure the new PAT version is set by running:
   Windows: %uepmdir%\bin>uepm patver get
   SecurePlatform and Gaia: $UEPMDIR/bin>uepm patver get
Chapter 11

Full Disk Encryption Policy

In This Section:

Overview of Full Disk Encryption ................................................................. 84
Full Disk Encryption Rule Actions ............................................................... 84
Full Disk Encryption Installation and Deployment ....................................... 90
Full Disk Encryption Recovery .................................................................. 92
Upgrading Full Disk Encryption ................................................................. 93
Full Disk Encryption Troubleshooting ......................................................... 94

Check Point Full Disk Encryption gives you the highest level of data security. It combines boot protection with Pre-boot authentication, and strong encryption to ensure that only authorized users can access data stored in desktop and laptop PCs.

Overview of Full Disk Encryption

Full Disk Encryption includes two main components:

- **Disk encryption** - 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** - Users must authenticate to their computers in the Pre-boot, 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 Full Disk Encryption in SmartEndpoint in the Policy tab > Full Disk Encryption Rules.

Make sure to configure the OneCheck User Settings Policy also in the Policy tab > OneCheck User Settings Rules. Many of the settings that relate to the Pre-boot are configured there.

Full Disk Encryption Rule Actions

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 to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.
**Disk Encryption**

These actions define if the volumes of the hard disk are encrypted or not.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt all local hard disks</td>
<td>All volumes of the hard disk are automatically fully encrypted. The encrypted disk is only accessible to authorized users.</td>
</tr>
<tr>
<td>Do not encrypt local hard disks - Encrypt only minimum volumes required for Pre-boot</td>
<td>The hard disk is not encrypted, except for a small section that is reserved for Pre-boot authentication.</td>
</tr>
</tbody>
</table>

Double-click an action to edit the properties.

- **Volume encryption algorithm:**
  Full Disk Encryption can use these encryption algorithms:
  - AES (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, you can 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.

**Authentication before Operating System (Pre-boot)**

These actions define 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.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate user before OS loads (Pre-boot)</td>
<td>Users must authenticate to their computers in the Pre-boot before the operating system loads.</td>
</tr>
</tbody>
</table>
| Do not authenticate user before OS loads (disable Pre-boot) | Users authenticate to their computers only at the operating system level.  
Note: This is less secure. 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**, you can choose to bypass Pre-boot in specified situations:

- **Bypass Pre-boot 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 (http://supportcontent.checkpoint.com/documentation_download?ID=24827).
- **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.
- **Temporary Pre-boot Bypass (Wake on LAN) settings** - For scenarios when you want to temporarily bypass the Pre-boot, for example, for maintenance, see Temporary Pre-boot Bypass (on page 86). Temporary Pre-boot Bypass reduces security.

If you choose **Do not authenticate user before OS loads (disable Pre-boot)**, the user experience is simpler, but it is less secure. As an alternative to Pre-boot Bypass, you can use Single Sign-On (SSO) together with Pre-boot Authentication.

If you do choose **Do not authenticate user before OS loads (disable Pre-boot)** we recommend that you require Pre-boot authentication in some scenarios. See Temporarily Require Pre-boot (on page 87).

**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.

**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 settings**.
3. Configure these options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Endpoint will disable Temporary Pre-boot Bypass after (number of automatic logons)</td>
<td>Enter the number of times the Temporary Pre-boot Bypass functionality can be used. After the number of logons expires, Temporary Pre-boot Bypass is disabled on the client and the Pre-boot environment shows.</td>
</tr>
<tr>
<td>The Endpoint will disable Temporary Pre-boot Bypass after (number of days)</td>
<td>Enter the number of days for which Temporary Pre-boot Bypass functionality is enabled. After the number of days 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.</td>
</tr>
<tr>
<td>Automatic logon starts after (number of minutes)</td>
<td>Enter the time delay in minutes. After the delay expires, Temporary Pre-boot Bypass logs the user into the Windows environment. During the delay, the Pre-boot Login window shows. The user can manually logs into the windows environment.</td>
</tr>
<tr>
<td>Allow OS Logon</td>
<td>Lets the user log in to OS after the Temporary Pre-boot Bypass logon.</td>
</tr>
</tbody>
</table>

Notes - 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.

**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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than X failed logon attempts were made</td>
<td>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.</td>
</tr>
<tr>
<td>The hard disk is not used by the original computer (hardware Hash)</td>
<td>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.</td>
</tr>
<tr>
<td>The computer cannot reach any of the configured locations</td>
<td>To make sure that the client is connected to the correct network, the computer pings a defined number of IP addresses during the boot process. If none of the IP addresses replies in a timely manner, the computer might have been removed from the trusted network and Pre-boot is required. The computer reboots automatically and the user must authenticate in Pre-boot.</td>
</tr>
<tr>
<td>Before Pre-boot authentication is required, show this message</td>
<td>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.</td>
</tr>
</tbody>
</table>
Full Disk Encryption Policy

Note - If a dynamic event fails, such as a Network Location Awareness Verification, the computer will not be able to reach configured locations.

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.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable USB device in Pre-boot environment (BIOS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Enable PCMCIA (BIOS only)</td>
<td>Enables the PCMCIA Smart Card reader. If you use Smart Cards that require this, make sure it is enabled.</td>
</tr>
<tr>
<td>Enable mouse in Pre-boot environment (BIOS only)</td>
<td>Lets you use a mouse in the Pre-boot environment.</td>
</tr>
<tr>
<td>Allow low graphics mode in Pre-boot environment (BIOS only)</td>
<td>Select to display the Pre-boot environment in low-graphics mode.</td>
</tr>
</tbody>
</table>
| 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 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. |
**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.

If user acquisition is enabled, users are prompted to log out and log in again so their accounts can be acquired for Pre-boot authorization. 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.

**OneCheck Logon**

OneCheck Logon is a Single Sign-On solution that let users log on one time to authenticate to:

- Full Disk Encryption
- DLP
Full Disk Encryption Policy

- 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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable lock screen authentication (OneCheck)</td>
<td>Users log on one time to authenticate to the operating system, Full Disk Encryption, and other Endpoint Security blades.</td>
</tr>
<tr>
<td>Enable OneCheck Identity Single Sign On for OS</td>
<td>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.</td>
</tr>
<tr>
<td>Use native sign on for OS</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

Double-click an action to edit the Properties.

**To configure OneCheck Logon properties:**

1. Select **Enable 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.

**Full Disk Encryption Installation and Deployment**

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

Clients must have:

- 32MB of continuous free space on the client's system volume

  **Note** - During deployment of the Full Disk Encryption blade 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
- On Windows XP, the root directory cannot be compressed. Subdirectories of the root directory can be compressed.

Completing Full Disk Encryption Deployment on a Client

Users will have 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.

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
- **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

Primary Full Disk Encryption Components

<table>
<thead>
<tr>
<th>Component Name</th>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption service</td>
<td>FDE_srv.exe</td>
<td>The Full Disk Encryption service contains the current configuration data and initiates background encryption or decryption. By exchanging volume boot records, the Full Disk Encryption service identifies volumes that are targeted for encryption.</td>
</tr>
<tr>
<td>Crypto core</td>
<td>ccore32.bin</td>
<td>The Crypto core contains the encryption algorithms.</td>
</tr>
</tbody>
</table>
Full Disk Encryption

Component Name | File Name  | Description
-----|------------|---------------------------------------------------
Filter driver | Prot_2k.sys | The Full Disk Encryption driver for encryption. The File Allocation Table (FAT) provides the driver with the location of sectors where data is stored. Full Disk Encryption encrypts every byte of the selected disk. Background encryption starts from the first sector of the selected volume and moves in sequence to the last sector. The entire operating system is encrypted.

Full Disk Encryption Recovery

If system failure prevents the operating system from starting on a client computer, Full Disk Encryption has these options:

- Full recovery with recovery media (on page 92) - 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.
- Dynamic Mount Utility (on page 93) - 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.

Full Recovery with Recovery Media

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 SmartEndpoint, 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:
     (i) Click Add to create a temporary user who can use the recovery media.
     (ii) 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 from the external recovery media tool on R77.20 and higher Management:
1. On an Endpoint Security Management Server, go to folder: C:\Program Files\CheckPoint\Endpoint Security\Full Disk Encryption\n2. Right-click UseRec.exe and select Run as > Administrator.
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.

Dynamic Mount Utility

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. Do the procedures in Upgrading Clients to E80.50.
**What effect does an upgrade have on users?**
The upgrade does not have a significant effect on users.

---

**Full Disk Encryption Troubleshooting**
This section covers basic troubleshooting.

**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

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

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 Technical Support for analysis.

The Client debug log is named dlog1.txt, and found in these places on user:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Path to log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\All Users\Application Data\CheckPoint\Endpoint Security\Full Disk Encryption</td>
</tr>
<tr>
<td>Windows Vista and higher</td>
<td>C:\ProgramData\CheckPoint\Endpoint Security\Full Disk Encryption</td>
</tr>
</tbody>
</table>

Pre-boot Issues

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** (http://supportcontent.checkpoint.com/documentation_download?ID=24827).

**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**

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 step.

**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.
   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.
Full Disk Encryption Policy

- Check the Security Package key.

To check the Security Package key:
1. Start Regedit.
2. Go to \HKLM\SYSTEM\CurrentControlSet\Control\LSA
3. Make sure that the Security Package key starts with one of these:
   - eps_kerberos_proxy
   - eps_msv_proxy
4. If it contains the default Kerberos msv1_0, change it to one of the correct values above.

Problem: The deployment is stuck at the encryption.

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.
Chapter 12

OneCheck User Settings Policy

In This Section:

- Overview of OneCheck User Settings ............................................................... 98
- OneCheck User Settings Policy Actions ............................................................. 98
- Before You Configure Smart Card Authentication ......................................... 103
- Changing a User's Password ............................................................................ 105

OneCheck User Settings defines the settings for user authentication to Endpoint Security client computers.

Overview of OneCheck User Settings

OneCheck User Settings includes:

- 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.

OneCheck User Settings Policy Actions

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 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.

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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate users with Password</td>
<td>Users can only authenticate with a username and password.</td>
</tr>
<tr>
<td>Authenticate users using Smart Card or Password</td>
<td>Users can authenticate with either username and password or Smart Card.</td>
</tr>
</tbody>
</table>

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 103). 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 (http://supportcenter.checkpoint.com).
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.
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. Clear Use Default Pre-boot Authentication Method and then click Modify.
5. Select an authentication method:
   - **Password** - This user can only authenticate with a username and password.
   - **Smart Card (requires certificate)** - 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.
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. Click OK.
8. 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**
These Actions define the requirements for user passwords for OneCheck User Settings:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Windows password complexity</td>
<td>The standard Windows password requirements are enforced:</td>
</tr>
<tr>
<td></td>
<td>The password must:</td>
</tr>
<tr>
<td></td>
<td>- Have at least six characters</td>
</tr>
<tr>
<td></td>
<td>- Have characters from at least 3 of these categories: uppercase, lowercase, numeric characters, symbols.</td>
</tr>
<tr>
<td>Use custom password complexity</td>
<td>If you select this, select the requirements for which type of characters the password must contain or not contain.</td>
</tr>
</tbody>
</table>

Double-click an action to edit the properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use custom requirements</td>
<td>If you select this, select the requirements for which type of characters the password must contain or not contain:</td>
</tr>
<tr>
<td></td>
<td>- Consecutive identical characters, for example, aa or 33</td>
</tr>
<tr>
<td></td>
<td>- Require special characters. These can be: ! * # $ % &amp; '( ) + , - . / : &lt; = &gt; ? @ {</td>
</tr>
<tr>
<td></td>
<td>- Require digits, for example 8 or 4.</td>
</tr>
<tr>
<td></td>
<td>- Require lower case characters, for example g or t.</td>
</tr>
<tr>
<td></td>
<td>- Require upper case characters, for example F or G.</td>
</tr>
<tr>
<td></td>
<td>- Password must not contain user name or full name.</td>
</tr>
<tr>
<td>Minimum length of password</td>
<td>Enter the minimum number of characters for a valid password.</td>
</tr>
<tr>
<td>Password can be changed only after</td>
<td>Enter the minimum number of days that a password must be valid before the user can change it.</td>
</tr>
</tbody>
</table>
**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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Pre-boot password Upon Windows Password Change</td>
<td>When the OS password on a computer changes, the Pre-boot password is automatically changed.</td>
</tr>
<tr>
<td>Update Windows Password Upon Pre-boot Password Change</td>
<td>When the Pre-boot password on a computer changes, the OS password is automatically changed.</td>
</tr>
<tr>
<td>Bi-directional Update for Pre-boot and Windows Password Upon Change</td>
<td>If the Pre-boot or OS password on a computer changes, the password is automatically changed.</td>
</tr>
<tr>
<td>Do Not Synchronize Pre-boot and Windows passwords</td>
<td>The Pre-boot and OS passwords on a computer are not synchronized by Endpoint Security.</td>
</tr>
</tbody>
</table>

**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:
OneCheck User Settings Policy

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not lock out users upon failed authentication.</td>
<td>Users are not locked out of their accounts if they try to log on unsuccessfully. This setting is not recommended.</td>
</tr>
<tr>
<td>Temporarily lock user account upon failed authentication attempts</td>
<td>After a configured amount of failed log on attempts (the default is 5), the user's account is temporarily locked.</td>
</tr>
<tr>
<td>Permanently lock user account upon failed authentication attempts</td>
<td>After a configured amount of failed log on attempts (the default is 10), the user's account is permanently locked.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of failed logons before the account is locked</td>
<td>Maximum number of failed logon attempts allowed before an account is permanently locked. The account is locked until an administrator unlocks it.</td>
</tr>
<tr>
<td>Number of failed attempts before a temporary lockout</td>
<td>Maximum number of failed logon attempts before an account is temporarily locked out.</td>
</tr>
<tr>
<td>Duration of a temporary lockout</td>
<td>Duration of a temporary lockout period, in minutes.</td>
</tr>
<tr>
<td>Maximum number of successful logons allowed before the account is locked</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow account to receive remote password change help</td>
<td>Let users get help from an administrator to reset the account password (for example, if the user forgets the password).</td>
</tr>
<tr>
<td>Allow account to receive One-Time Logon help</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 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)**.
OneCheck User Settings Policy

- 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, as described in the **Installing and Deploying Endpoint Security Clients** chapter. 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 users 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.

\[\text{Note} - \text{You can put all Smart Card users in a virtual group so that it is easy to monitor them and change their policies, if necessary.}\]

**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.

---

End of document
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.
Chapter 13

Media Encryption & Port Protection Policy

In This Section:

- Media Encryption & Port Protection Terminology ................................................... 106
- Overview of Media Encryption & Port Protection ..................................................... 106
- Working with Actions in a Rule .............................................................................. 107
- Converting File Encryption Devices to Media Encryption .................................... 122

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. Examples include: keyboards, Bluetooth devices and Smart Card readers.

**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. Examples include: word processor files, spreadsheet files, presentations, and drawings.

**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 blade is not active or not connected to an Endpoint Security Management Server.

Overview of Media Encryption & Port Protection

The Media Encryption & Port Protection blade 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.
See the E80.50 Client User Guide for more information about how users interact with Media Encryption & Port Protection.

Working with Actions in a Rule

Each Media Encryption & Port Protection rule includes these main action types:

- **Read Action** ("Configuring the Read Action" on page 107) - Controls how users can read devices that are protected by the policy
- **Write Action** ("Configuring a Write Action" on page 108) - Controls how and when users can write to devices that are protected by the policy
- **Peripheral Device Access** ("Configuring Peripheral Device Access" on page 110) - Controls access to different types of peripheral devices

Media Encryption & Port Protection rules also contain these **Advanced** action types:

- **Offline Device Access** ("Offline Access Actions" on page 114) - Controls access to devices that are connected to a non-protected computer
- **Log Actions** (on page 117) - Controls when Media Encryption & Port Protection creates log entries when a storage device is attached to an endpoint computer
- **UserCheck** ("UserCheck Actions" on page 118) - Controls when and how to tell users about policy violations and optionally lets them override a policy.
- **Site Actions** ("Media Encryption Site Actions" on page 119) - Controls when to allow or prevent access to drives encrypted by different Endpoint Security Management Servers
- **Global Automatic Access** ("Global Automatic Access Action" on page 120) - 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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow reading any data from storage devices</td>
<td>Allow users to read encrypted and non-encrypted data from storage devices.</td>
</tr>
<tr>
<td>Allow reading only encrypted data from devices</td>
<td>Allow users to read only encrypted data from storage devices. Users cannot read unencrypted (Non-Business related) data.</td>
</tr>
<tr>
<td>Do not allow reading from any storage device</td>
<td>Block reading from all storage devices.</td>
</tr>
</tbody>
</table>

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 plain 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 Settings for Specified Devices ("Defining Exceptions for Devices " on page 111).

**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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow writing any data to storage devices</strong></td>
<td>Users can write all file types to storage devices.</td>
</tr>
<tr>
<td><strong>Encrypt business related data written to storage devices</strong></td>
<td>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 109).</td>
</tr>
<tr>
<td><strong>Encrypt all data written to storage devices</strong></td>
<td>All files written to a storage device must be encrypted. This includes both Business and Non-Business Related data.</td>
</tr>
<tr>
<td><strong>Do not allow writing any data to storage devices</strong></td>
<td>Users cannot write any file types to storage devices.</td>
</tr>
<tr>
<td><strong>Do not allow writing any data to storage devices, allow user override</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 select the Do not log 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.
Media Encryption & Port Protection Policy

Click Additional Encryption Options to configure additional encryption settings ("Offline Access Actions" on page 114) as necessary.

- **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 ("Creating a Custom User Message" on page 110) to create your own user message.

  **Note** - The **Allow user to override company policy** option is not supported for CD/DVD ROM devices.

6. If necessary, click Configure file ("Configuring Business Related File Types" on page 109) types to define custom business related file types.

### 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.

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.
- **Text** - Plain text files
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.
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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow connecting essential devices (keyboard, mouse, and network adapters)</td>
<td>Access to necessary peripheral devices for basic computer functionality is allowed. Other peripheral devices are blocked.</td>
</tr>
<tr>
<td>Block all transmitting devices (Modem, Bluetooth, IrDA, Wi-Fi)</td>
<td>Access to transmitting peripheral devices is blocked. Other peripheral devices are allowed.</td>
</tr>
<tr>
<td>Allow connecting all peripheral devices</td>
<td>Access to all devices that cannot be encrypted or do not contain storage is allowed.</td>
</tr>
</tbody>
</table>

You can also create ("Creating a Custom Action" on page 110) and change ("Changing an Existing Action" on page 111) 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 Information**
  - 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 ("Using Wild Card Characters" on page 113) in the serial number to apply this device definition to more than one physical device.
  - Extra Information - Configure if the device shows as a hard disk drive (Hard Drive with Master Boot Record), a device with removable storage (Media without Master Boot Record) or other type (None).
  - Icon - Select an icon to show in the GUI.

- **Device ID Filter**
  - Device ID begins with - Enter a filter string that identifies the device model (hardware ID). 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_2MB
My_USB Stick_4MB
```

- **Capabilities**
  - Supports encryption of media - Select this option if the device can be encrypted (storage devices only).
- **Supports generation of audit logs upon detection** - 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 (“Editing Device Details” on page 111).
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 108).
   - For Storage Device Read Access see Configuring the Read Action (on page 107).
   - 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 111).
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 108).
   - For Storage Device Read Access see Configuring the Read Action (on page 107).
   - 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 108).
   - For Storage Device Read Access see Configuring the Read Action (on page 107).
   - 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 ("Editing Device Details" on page 111) as necessary.

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:

<table>
<thead>
<tr>
<th>Serial Number with Wildcard</th>
<th>Matches</th>
<th>Does Not Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234*</td>
<td>1234AB, 1234BCD, 12345</td>
<td>1233</td>
</tr>
<tr>
<td>1234??</td>
<td>1234ABC, 1234XYZ, 1234567</td>
<td>1234AB, 1234x, 12345678</td>
</tr>
</tbody>
</table>

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????
**Advanced Actions**

**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:

<table>
<thead>
<tr>
<th>Encryption Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setting</strong></td>
</tr>
<tr>
<td>Allow user to choose owner during encryption</td>
</tr>
<tr>
<td>Allow user to change size of encrypted media</td>
</tr>
<tr>
<td>Allow users to remove encryption from media</td>
</tr>
<tr>
<td>Allow user to upgrade from legacy drives</td>
</tr>
<tr>
<td>When encrypting, Non-Business Related Data will be:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Secure format media before encryption</td>
</tr>
<tr>
<td>Change device name and icon after encryption</td>
</tr>
</tbody>
</table>
### Offline Access Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password protect media for access in offline mode</td>
<td>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</td>
</tr>
<tr>
<td>Allow user to recover their password using remote help</td>
<td>Lets users recover passwords using remote help.</td>
</tr>
<tr>
<td>Copy utility to media to enable media access in non-protected environments</td>
<td>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.</td>
</tr>
<tr>
<td>Protect media with password for read-only access in offline mode</td>
<td>Lets users assign a different password that gives read-only access to a storage device.</td>
</tr>
<tr>
<td>Allow user to change read-only password</td>
<td>Lets users change a previously defined read-only password.</td>
</tr>
</tbody>
</table>

### Password Constraints for Offline Access

In the Properties of the Offline Access action, click **Configure password constraints** to set the requirements for passwords used to access encrypted devices.

These Actions define the requirements for user passwords for Media Encryption & Port Protection:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Windows password complexity</td>
<td>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.</td>
</tr>
<tr>
<td>Use custom password complexity</td>
<td>If you select this, select the requirements for which type of characters the password must contain or not contain.</td>
</tr>
</tbody>
</table>

Double-click an action to edit the properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use custom requirements</td>
<td>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: ! * # $ % &amp;’ ( ) * + - . / : &lt; = &gt; ? @ {</td>
</tr>
<tr>
<td>Minimum length of password</td>
<td>Enter the minimum number of characters for a valid password.</td>
</tr>
<tr>
<td>Password can be changed only after</td>
<td>Enter the minimum number of days that a password must be valid before the user can change it.</td>
</tr>
<tr>
<td>Password expires after</td>
<td>Enter the maximum number of days that a password can be valid before the user must change it.</td>
</tr>
</tbody>
</table>
Media Encryption & Port Protection Policy

**Option** | **Description**
---|---
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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not lock out storage device upon failed authentication.</td>
<td>Users are not locked out of a device if they try to log on unsuccessfully. This setting is not recommended.</td>
</tr>
<tr>
<td>Temporarily lock storage device upon failed authentication attempts</td>
<td>After a configured amount of failed log on attempts (the default is 5), the device is temporarily locked.</td>
</tr>
<tr>
<td>Permanently lock storage device upon failed authentication attempts</td>
<td>After a configured amount of failed log on attempts (the default is 10), the device is permanently locked.</td>
</tr>
</tbody>
</table>

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.

You can select one of these predefined options for a Media Encryption & Port Protection rule:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require storage devices to be scanned and authorized. Allow self-authorization.</td>
<td>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.</td>
</tr>
<tr>
<td>Require storage devices to be scanned and authorized. Do not allow self-authorization.</td>
<td>Scan the device when inserted. Specified administrators must authorize the device after a successful scan.</td>
</tr>
<tr>
<td>Do not scan storage devices</td>
<td>Storage devices are not scanned when inserted and no authorization is necessary.</td>
</tr>
<tr>
<td>New</td>
<td>Create a custom action with different authorization and media scan requirements.</td>
</tr>
</tbody>
</table>

You can configure which file types can or cannot be on storage devices.

**To configure which file types can be on storage devices:**

1. 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**.

**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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique action name.</td>
</tr>
<tr>
<td>Comments</td>
<td>Optional textual comments.</td>
</tr>
<tr>
<td>Scan storage devices and authorize them for access</td>
<td>Select to scan the device when inserted. Clear to skip the scan.</td>
</tr>
<tr>
<td>Enable self-authorization</td>
<td>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.</td>
</tr>
<tr>
<td>Automatic media authorization</td>
<td>The device is authorized automatically.</td>
</tr>
<tr>
<td>Allow user to delete unauthorized files.</td>
<td>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.</td>
</tr>
<tr>
<td>Manual media authorization</td>
<td>Users or administrator must manually authorize the device.</td>
</tr>
<tr>
<td>Allow user to skip media scan</td>
<td>The user can optionally skip the scan when a device is connected to a client.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not log security events</td>
<td>Disable all log entries.</td>
</tr>
<tr>
<td>Log only critical events</td>
<td>Create log entries only for events that are classified as critical.</td>
</tr>
<tr>
<td>Log critical and security events</td>
<td>Create log entries only for events that are classified as critical or security events.</td>
</tr>
</tbody>
</table>
Media Encryption & Port Protection Policy

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log all events</td>
<td>Create log entries for all events.</td>
</tr>
</tbody>
</table>

You cannot define custom log actions.

This table shows the applicable Media Encryption & Port Protection events and their severity classification.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Policy update completed successfully</td>
<td>Low</td>
</tr>
<tr>
<td>7</td>
<td>Device authorization successful</td>
<td>Low</td>
</tr>
<tr>
<td>8</td>
<td>Device authorization failed</td>
<td>Critical</td>
</tr>
<tr>
<td>11</td>
<td>Device access is blocked when attached to the endpoint computer</td>
<td>Critical</td>
</tr>
<tr>
<td>15</td>
<td>Encrypted storage created successfully</td>
<td>Low</td>
</tr>
<tr>
<td>16</td>
<td>Encrypted storage device removed</td>
<td>Critical</td>
</tr>
<tr>
<td>20</td>
<td>Device is attached to an endpoint computer and access is allowed</td>
<td>Security</td>
</tr>
<tr>
<td>21</td>
<td>A user follows the Ask User procedure to override a rule</td>
<td>Critical</td>
</tr>
<tr>
<td>22</td>
<td>A user does not follow the Ask User procedure to override a rule</td>
<td>Critical</td>
</tr>
<tr>
<td>23</td>
<td>A storage device file operation is blocked</td>
<td>Critical</td>
</tr>
<tr>
<td>24</td>
<td>A storage device file operation is allowed</td>
<td>Security</td>
</tr>
</tbody>
</table>

You can define different log settings for specified devices ("Defining Exceptions for Devices" on page 111). 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 & Port Protection Policy

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".

<table>
<thead>
<tr>
<th>The client is connected to:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The encrypting Endpoint Security Management Server</td>
<td>User can access automatically or enter a password for access.</td>
</tr>
<tr>
<td>A different trusted Endpoint Security Management Server</td>
<td>User can enter a password for access.</td>
</tr>
<tr>
<td>A non-trusted Endpoint Security Management Server</td>
<td>User cannot access the device.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to media encrypted at current site only</td>
<td>Media Encryption Site (UUID) verification is enabled. Endpoint Security clients can only access encrypted devices that were encrypted by the same or another trusted Endpoint Security Management Server.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted storage devices are fully accessible by all users</td>
<td>All users can read and change all encrypted content.</td>
</tr>
<tr>
<td>All users in the organization can read encrypted data, only owners can modify</td>
<td>All users can read encrypted files on storage devices. Only the media owner has can change encrypted content.</td>
</tr>
<tr>
<td>Only owners can access encrypted data</td>
<td>Only media owners read and/or change encrypted content.</td>
</tr>
<tr>
<td>Access to encrypted data requires password authentication</td>
<td>Users must enter a password to access the device. Automatic access in not allowed.</td>
</tr>
</tbody>
</table>

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
Media Encryption & Port Protection Policy

• 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.

Upgrading Media Encryption R73.x Devices and Keys

This version includes a wizard that lets you export Media Encryption devices from the R73.x database and import them into an E80.50 Endpoint Security Management Server. When upgrading from Media Encryption R73 to the current version:

• We recommend that you add the UUID of the R73 server to the trusted list.
• You can access devices that were encrypted on the R73 Media Encryption server automatically, if you export the devices and keys from the R73 database and import them in to the Endpoint Security Management Server.

⚠️ Important - Encryption keys associated with Active Directory users that were not added to the Media Encryption (Protector) server manually or through group synchronization, will not be migrated.

Media Encryption (Protector) Encryption Keys and Devices are stored in the MS-SQL database. The Protector Server connects to MS-SQL through named pipelines. To migrate Media Encryption keys and devices, you must configure MS-SQL to accept requests over TCP connections. You must create a login profile that has the permissions required to access the Disknet database.

• If the Protector Server is installed with default settings, use the instructions here.
• If the MS-SQL is installed on an external machine, or MS-SQL management tools are installed, consult with your DBA, and skip to the Running Migration Tools section.

To configure the MS-SQL server to accept requests over TCP connections:

1. In the regedit tool, find the "SuperSocketNetLib" key.
   The path to this key can be different according to the platform and installed tools.
2. Right-click the "SuperSocketNetLib" entry and export it for backup.
3. Create a reg file to customize the server:
   If the path to the SuperSocketNetLib entry is the same in the Media Encryption (Protector) server and in this article:
   a) Copy this registry fragment to a separate file.
   b) Save it with the "reg" extension, and run it.
   If the path is different, edit the new reg file so that it fits the path on the machine.

```plaintext
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer]
"LoginMode"=dword:00000002
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib]
"ProtocolList"=hex(7):74,00,63,00,70,00,00,00,6e,00,70,00,00,00,00,00,00,00
"TcpPort"="1433"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib]
"ProtocolList"=hex(7):74,00,63,00,70,00,00,00,6e,00,70,00,00,00,00,00,00,00
"TcpPort"="1433"
```

Media Encryption R73.x Devices and Keys - Upgrade Instructions
4. When the registry edit is done, open the regedit utility.
5. Make sure that the "reg" script ran successfully and that the values in the registry were changed according to the script.
6. Restart the "MSSQLSERVER" process.

**To add a new login profile to the MS-SQL server:**
1. Run the osql tool from the command line: `osql -E`
2. Run these commands in the osql command line:

   ```
   EXEC sp_addlogin 'ep','ep'
   GO
   EXEC sp_grantdbaccess 'ep', 'Disknet'
   GO
   EXEC sp_addsrvrolemember 'ep', 'sysadmin'
   GO
   ```

**To run the Migration Wizard:**
1. Make sure that Media Encryption & Port Protection and the Endpoint Security server are up and running.
   **Important!** This is required to complete the key migration successfully.
3. Open the SmartEndpoint console.
4. Click **Tools** menu > **Devices and Keys Migration Tool**.
5. Enter the details of the Media Encryption R73 Database: IP address or server name, Database Username, Database Password, Database Name.
6. Click **Next**.
7. Select **Import Devices** or **Import Keys** or both.
8. Click **Next**.
   See the import results. When import is done, users can access the media from computers with Endpoint Security client installed.
   **Important!** Users must access the media at least once to enable Remote Help Key Recovery.

   More details can be found in `deviceMigrtor.log` file, which is located in the same folder as the `SmartEndpoint.exe` executable. To go to this folder, right-click the `SmartEndpoint` icon and select **Properties** > **Open File Location**.

---

### Converting File Encryption Devices to Media Encryption

You can easily convert storage devices that were encrypted with Pointsec File Encryption R73 and earlier to Media Encryption E80.xx. When you insert a device encrypted with Pointsec File Encryption into an endpoint computer running this version, you are prompted to upgrade the device.

**To convert a File Encryption device to Media Encryption:**
1. Insert the device into a computer that has an Endpoint Security client with the Media Encryption & Port Protection blade active.
2. This message shows:
   **To access the device, you need to convert it to Media Encryption format.**
3. Click **OK**.
4. If necessary, enter the **File Encryption credentials of the device** in the window that opens. These must be the credentials originally to encrypt the storage device. They can be:
   - A corporate user name and password assigned by the administrator
   - A personal user name and password defined for this storage device
If the device was originally encrypted with a corporate password and Media Encryption & Port Protection can find the password on the computer, this window does not open.

5. Enter and re-enter a new password for the device.
6. Click **Continue**.
7. Optionally, edit the Media Encryption settings.
8. Click **Encrypt**.
9. When the encryption is complete, click **Finish**.
Chapter 14

Anti-Malware Policy

In This Section:

Prerequisites ........................................................................................................................................ 124
Anti-Malware Policy Actions .................................................................................................................. 125
Submitting Malware and False Detections .......................................................................................... 128

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

Before configuring Anti-Malware, you must:

- Configure a proxy server if you plan to use Anti-Malware in an environment that includes a proxy server for Internet access.
- Configure the firewall gateway to accept traffic from Anti-Malware updates.
- Configure port access.

To configure the Endpoint Security Management Server to work with a proxy server:

2. Open %uepmdir%\engine\conf and edit the local.properties file.

   Note - Delete the #character from the beginning of each row that you edit.

3. Add these properties:

   a) The proxy server’s IP address as shown in the example below:
      
      http.proxy.host=<IP address>

   b) The proxy server’s listening port as shown in the example below:
      
      http.proxy.port=8080

   c) The username if basic authentication is enabled on the proxy server. Leave it empty if no authentication is required.
      
      http.proxy.user=<username>

   d) The password if basic authentication is enabled on the proxy server.
      
      http.proxy.password=<password>

4. Save the %uepmdir%\engine\conf\local.properties file.
Allowing Anti-Malware Update Traffic

After configuring the proxy server, configure the firewall gateway to accept the traffic to the update servers.

To enable update traffic through a proxy server:
1. In your firewall gateway, allow outbound internet connectivity.
2. In your firewall gateway, allow outbound connectivity to the Anti-Malware update server.

Port Access

The Endpoint Security server must have access to ports 80 and 443 to retrieve the latest malware definitions. Make sure that your firewall gateway allows this traffic.

Anti-Malware Policy Actions

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 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.

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for malware signature updates every 4 hours</td>
<td>Signature updates occur every 4 hours from the Endpoint Policy Server and Check Point server.</td>
</tr>
<tr>
<td>Check for malware signature updates every 2 hours</td>
<td>Signature updates occur every 2 hours from the Endpoint Policy Server and Check Point server.</td>
</tr>
</tbody>
</table>

Double-click an Action to edit the Properties.

You can change these settings:

- **Updater Interval** - Frequency, in hours, between client requests for malware signatures and scanning for engine updates.
- **Updater Timeout** - The connection time out, after which the update source is considered unavailable.
• **Signature Update Server** - The server or servers that the client gets updates from.
• **Update from the Endpoint policy server** - Get updates from the Endpoint Security Management Server or configured Endpoint Policy Server.
• **Update signatures from Check Point server** - Get updates from an external Check Point server through the internet: The default URL is: [http://kav8.zonealarm.com](http://kav8.zonealarm.com).
• **Update signatures from external source** - Get updates from an external source through the internet. Enter the URL.

If you select all options, the client first tries to get updates from the Endpoint Policy Server. If the server is unavailable, the client downloads updates from the external Check Point server. If the client cannot connect to the external Check Point server, it tries the manually configured URL.

**Note** - If only the first option is selected, clients that are disconnected from an Endpoint Security server cannot get updates.

### Schedule of Malware Scans

Anti-Malware scans computers for malware at regular intervals to make sure that suspicious files are treated, quarantined, or deleted.

These Actions define the frequency of the scans.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform periodic anti-malware scan every day</td>
<td>A scheduled scan occurs every day at the time shown in the Properties.</td>
</tr>
<tr>
<td>Perform periodic anti-malware scan every week</td>
<td>A scheduled scan occurs every week at the day and time shown in the Properties.</td>
</tr>
<tr>
<td>Perform periodic anti-malware scan every month</td>
<td>A scheduled scan occurs every month at the date and time shown in the Properties.</td>
</tr>
</tbody>
</table>

Double-click an Action to edit the **Properties**.

You can select the exact day and time of day that the scan occurs.

The targets of the scan are defined in the **Scheduled Scan Targets** Action.

### Periodic Scan Options

These Actions define which components of computers are scanned during the scheduled malware scans.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodically scan system critical areas only</td>
<td>The scheduled scan scans system critical areas, for example: the operating system, processes, and memory. These are the targets of most malicious programs.</td>
</tr>
<tr>
<td>Periodically scan local hard-drives</td>
<td>The scheduled scan scans system critical areas and local drives.</td>
</tr>
<tr>
<td>Periodically scan local and removable drives</td>
<td>The scheduled scan scans system critical areas and local and removable drives.</td>
</tr>
</tbody>
</table>

Double-click an Action to edit the Properties.

You can change:

- The exact scan targets.
- Files or folders that are excluded from scans.
- **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, Scheduled scans and Contextual 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. The options are:

Do not optimize malware scan - Scan optimization is disabled.

Optimize malware scan - Enables the Perform scan optimizations feature only (see below).

You can define custom scan optimization actions by enabling these options:

- 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.
• **Scan Priority is lower than other running process** - Makes sure that scans have a lower priority for CPU, disk and other I/O resources to minimize the performance impact on critical processes.

**Malware Treatment**

The malware treatment options let you choose what happens to malware that is detected on a client computer. The options are:

- **Quarantine detected malware** - 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 detected malware** - If Endpoint Security cannot repair the file, it is deleted.

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.

**Exceptions**

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.

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 Smart Log

**To create a list of exceptions for malware treatment:**

1. In the Edit Properties - Malware Treatment window, click Override treatment for specific infections.
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.
Chapter 15

Firewall Policy

In This Section:

- Planning Firewall Policy ........................................................................................ 129
- Inbound Traffic Rules ............................................................................................ 129
- Outbound Traffic Rules ......................................................................................... 130
- Creating Firewall Rules ......................................................................................... 130
- Wireless Connection Settings ............................................................................... 132
- Hotspot Settings .................................................................................................... 132
- IPv6 Traffic ............................................................................................................ 132
- Choose a Firewall Policy to Enforce ..................................................................... 132

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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow inbound traffic</td>
<td>Allows all incoming traffic to the endpoint computer,</td>
</tr>
<tr>
<td>Allow inbound traffic from trusted zones and connectivity services</td>
<td>Allows all incoming traffic from trusted zones and IP obtaining traffic from the internet. All other traffic is blocked.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow any outbound traffic</td>
<td>Allows all outgoing traffic from the endpoint computer.</td>
</tr>
<tr>
<td>Allow outbound traffic to trusted zones and common internet protocols</td>
<td>Allow all traffic to trusted zones and traffic of common internet protocols to the internet.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule priority number</td>
<td>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.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Firewall Rule.</td>
</tr>
</tbody>
</table>
| 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**.        |
Firewall Policy

<table>
<thead>
<tr>
<th>Track</th>
<th>When the rule is enforced:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Log - Record rule enforcement in the Endpoint Client Log Viewer.</td>
</tr>
<tr>
<td></td>
<td>• Alert - Show a message on the endpoint computer and record rule enforcement in the Endpoint Client Log Viewer.</td>
</tr>
<tr>
<td></td>
<td>• None - Log and alert messages are not created.</td>
</tr>
</tbody>
</table>

Notes:

• If you have a rule that drops or accepts all traffic, do not enable logging.

• To use logs and alerts, Log upload to servers must be allowed in the Client Settings rule.

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 SmartDashboard. When you create a new object, it is also available in SmartDashboard. If you change an object in the SmartEndpoint or SmartDashboard, 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow connecting wireless to LAN</td>
<td>Users can connect to wireless networks while connected to the LAN.</td>
</tr>
<tr>
<td>Do not allow connecting wireless to LAN</td>
<td>Users cannot connect to wireless networks while connected to the LAN.</td>
</tr>
</tbody>
</table>

Hotspot Settings
These actions define if users can connect to your network from hotspots in public places, such as hotels or airports.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow hotspot registration</td>
<td>Bypass the firewall to let users connect to your network from a hotspot.</td>
</tr>
<tr>
<td>Do not allow hotspot registration</td>
<td>Do not let users connect to your network from a hotspot.</td>
</tr>
</tbody>
</table>

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

Choose 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 SmartDashboard.

Select which Firewall policy to enforce:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce the above Firewall policy</td>
<td>Use the Endpoint Security Firewall Policy Rules</td>
</tr>
<tr>
<td>Enforce Desktop Policy from SmartDashboard</td>
<td>Use the Desktop Policy from SmartDashboard</td>
</tr>
</tbody>
</table>

To activate the Desktop Policy from SmartDashboard:
1. Select Enforce Desktop Policy from SmartDashboard.
2. Install Policy.
3. Restart all computers included in the rule.
Chapter 16

Compliance Policy

In This Section:

Overview of Compliance ................................................................. 133
Planning for Compliance Rules ......................................................... 133
Compliance Policy Actions ............................................................... 134
Monitoring Compliance States ......................................................... 138
The Heartbeat Interval ..................................................................... 139

The Compliance blade 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.

Overview of Compliance

Compliance makes sure that:

- All assigned Software Blades 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 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 Mac.

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 (“Enforcing Rules According to States” on page 58).

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.
4. Define rule alerts and login policies to enforce the rules after deployment.

**Compliance Policy Actions**

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** to change the Action behavior.

Changes to policy rules are enforced only after you install the policy.

**Blades Running Action**

This action makes sure that all installed Software Blades are running and defines what happens if they are not running. The action options are:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inform if assigned Software Blades are not running</td>
<td>Send a warning message if one or more assigned blades are not running.</td>
</tr>
<tr>
<td>Restrict if assigned Software Blades are not running</td>
<td>Restrict network access if one or more assigned blades are not running.</td>
</tr>
<tr>
<td>Monitor if assigned Software Blades are not running</td>
<td>Create log entries if one or more assigned blades are not running. No messages are sent.</td>
</tr>
<tr>
<td>Do not check if assigned Software Blades are not running</td>
<td>The Compliance Blade does not make sure that assigned Software Blades are running.</td>
</tr>
</tbody>
</table>

**VPN Client Verification Action**

The VPN Client Verification action selects the procedure used to enforce the Upon verification failure option, as defined in SmartDashboard. The two 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 Remote Access Clients 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.

**Endpoint Security Analysis Report Action**

If the **Generate Endpoint Security Analysis Report** action is selected, the Endpoint Security Management Server generates an analysis report of all Endpoint Security clients in the environment. Each client sends information to the server one time each day and the information is summarized by the server hourly.

See the report in the Reporting tab > Endpoint Security Analysis Report.

The report includes:

- General data loss risk and computers with the highest risk of data loss.
- General unauthorized access risk and computers with the highest risk of unauthorized access.
• General threat risk and computers with the highest risk of threats.
This action is the same in all Compliance rules.

**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 blade 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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observe</td>
<td>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.</td>
</tr>
<tr>
<td>Warn</td>
<td>Alerts the user about non-compliance and automatically does the specified remediation steps. Send a log entry to the administrator.</td>
</tr>
<tr>
<td>Restrict</td>
<td>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.</td>
</tr>
</tbody>
</table>

The Compliance blade 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 rule ("Compliance Check Objects" on page 135).
   c) Select an Action from the list.
   d) Click the Remediation tab to add remediation objects to the rule ("Compliance Remediation Objects" on page 137). 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 blade 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for this Check Object.</td>
</tr>
<tr>
<td>Comment</td>
<td>Optional: Free text description</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the operating system that this Check object is enforced on.</td>
</tr>
</tbody>
</table>
| 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. |
| 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
<td></td>
</tr>
<tr>
<td>Run Custom File</td>
<td>Run the specified program or script when an endpoint computer is not compliant.</td>
</tr>
<tr>
<td><strong>Download Path</strong></td>
<td></td>
</tr>
<tr>
<td>• 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).</td>
<td></td>
</tr>
<tr>
<td>• This parameter is required.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td></td>
</tr>
<tr>
<td>• Enter the URL of an HTTP or file share server where the file is located.</td>
<td></td>
</tr>
<tr>
<td>• Enter the full path that includes the actual file with one of the supported extensions (*.bat or *.exe).</td>
<td></td>
</tr>
<tr>
<td>• This field can be left empty.</td>
<td></td>
</tr>
<tr>
<td>• Make sure the file share is not protected by a username or password.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>MD5 Checksum</strong></td>
<td>Click <strong>Calculate</strong> to generate a MD5 Checksum, a compact digital fingerprint for the installed application or the remediation files.</td>
</tr>
<tr>
<td><strong>Run as System</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Run as User</strong></td>
<td>Apply user rights and local environment variables for running the executable file.</td>
</tr>
<tr>
<td><strong>Messages</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Automatically execute operation without user notification</strong></td>
<td>Run the executable file without displaying a message on the endpoint computer.</td>
</tr>
<tr>
<td><strong>Execute operation only after user notification</strong></td>
<td>Run the executable file only after a user message opens and the user approves the remediation action. This occurs when <strong>Warn</strong> or <strong>Restrict</strong> is the selected action on a compliance check.</td>
</tr>
</tbody>
</table>
### Compliance Policy

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use same message for both Non-Compliant and Restricted messages</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Message Box</strong></td>
<td>Displays selected non-compliant and restricted messages. The message box is available only by selecting the Execute only after user notification setting. Click <strong>Add</strong>, <strong>Remove</strong>, or <strong>Edit</strong> to add a message, and remove or revise a selected message. <strong>Note</strong>: User cannot prevent the remediation application or file from running.</td>
</tr>
</tbody>
</table>

### 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 135) 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 135) for more information.

### Anti-Malware for Compliance

The **Anti-Malware for Compliance** 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 135) for more information.

### Service Packs for Compliance

The **Service Packs for 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 135) for more information.

### Monitoring Compliance States

Monitor the compliance state of computers in your environment from:

- **SmartView Tracker**
- **The Security Overview**
- **Reporting > Compliance**
Compliance Policy

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 ("Configuring the "About to be Restricted" State." on page 60).
- **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 computers send "heartbeat" messages to the Endpoint Security Management Server to make sure that all connections are active and that all policies are up to date. The time between heartbeat messages is known as the *heartbeat interval*.

**Note** - The default heartbeat interval is 60 seconds.

A heartbeat interval that is too short can cause performance degradation. A heartbeat interval that is too long can cause security degradation and less accurate reporting.

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.

**To configure the heartbeat interval:**
1. Click Manage > General Properties.
   The General Properties window opens.
2. In the Connection Settings section, set the Interval between client heartbeats.
3. 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. In the Endpoint Security console, select Manage > General Properties > Connection Settings.
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:

\[ \text{minutes} = \text{number of heartbeats} \times \text{heartbeat interval (in seconds)} \times 60. \]
Chapter 17

Application Control Policy

In This Section:

Working with the Application Control Policy ......................................................... 140
Reputation Service ................................................................................................ 141

The Application Control blade restricts network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes. Only applications that try to get network access can be blocked or terminated. If specified in an Application Control rule, an alert shows which application was blocked or terminated.

You can also enable the Reputation Service (previously called the Program Advisor) to recommend applications to allow or block.

Working with the Application Control Policy

Configure which applications are allowed, blocked, or terminated and what happens when applications are not identified.

To configure the allowed applications:
1. In the Policy tab > Application Control rule, right click the Allowed Apps Action and select Manage Allowed Apps List.
2. To add more applications, click Add and select applications from the Search Applications window.
3. Click OK.

To configure the blocked applications:
1. In the Policy tab > Application Control rule, right click the Block Apps Action and select Manage Blocked Apps List.
2. To add more applications, click Add and select applications from the Search Applications window.
3. Click OK.

To configure terminated applications:
1. In the Policy tab > Application Control rule, right click the Terminated Apps Action and select Manage Terminated Apps List.
2. To add more applications, click Add and select applications from the Search Applications window.
3. Click OK.

If you block unidentified applications, users can only access applications that are included in the Allowed Apps List. If you allow unidentified applications, users can access all applications that are not on the blocked or terminated list. If you choose to allow unidentified traffic, make sure your blocked and terminated lists are complete.

To configure what happens to unidentified applications:

In the Policy tab > Application Control rule, select Block Unidentified Applications, or right click and select Allow Unidentified applications.

Terminated applications are not allowed to pass through the firewall.
Reputation Service

The Check Point Reputation Service is an online service that automatically creates recommended rules that block or allow common applications. These rules are based on the recommendations of Check Point security experts. This feature reduces your workload while improving security and usability.

Note - Your 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 your firewall allows this traffic. We recommend that you add the Reputation Service Server to your Trusted Zone.

To see the recommendations of the Reputation Service for safe applications:
1. In the Application Control rule, right click the Allow Whitelisted Apps action and select Manage Allowed Apps List.
2. In the Allow Applications List, select Good Reputation from the options menu.
   A list of applications with a good reputation, generated by the Reputation Service, opens. You can move applications to the Block or Terminate list.

To see the recommendations of the Reputation Service for malicious applications:
1. In the Application Control rule, right click the Terminated Apps action and select Manage Terminated Apps List.
2. In the Terminate Application List, select Known Malware Apps from the options menu.
   A list of malicious applications, generated by the Reputation Service, opens. You can move applications to the Block or Allow list.

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 in Windows:
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.
**Importing Program References**

The Appscan command lets you automatically create Application Control rules for based on common applications and operating system files on endpoint computers network. This is especially useful when you have a clean standard image.

To import a list of programs identified by their checksums, instead of by filename. Checksums are unique identifiers for programs that cannot be forged. This prevents malicious programs from masquerading as other, innocuous programs.

Create an Appscan for each disk image used in your environment. You can then create rules that will apply to those applications. You create Appscan files by running the appscan.exe utility on a computer with a tightly-controlled disk image, then importing the file into Endpoint Security.

**Creating an Appscan XML File**

Before you can use Appscan, set up a Windows computer with the typical applications used on protected computers in your organization. If you have several different configurations, perform these steps for each.

!) **Important** - The computer you scan to create an Appscan must be free of all malware. If you are certain that your scan is clean, you can create rules that allow the applications access to the network.

To run Appscan from the command line:

1. Download the appscan tool from [sk82100](http://supportcontent.checkpoint.com/solutions?id=sk82100), to the root directory (typically c:\) of the baseline reference source computer.

   To run this utility on Window 95, 98, or ME operating systems, you also need to copy unicows.dll, located in the <installdir>checkpoint\Integrity\engine\webapps\ROOT\bin directory on the Endpoint Security host, to the root directory (typically c:\) of the baseline reference source computer.

   **Important** - Do not copy the unicows.dll file if the baseline reference source computer is running any operating system other than Windows 95, 98, or ME.

2. From the target computer command prompt, 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 (Default = scanfile.xml) is created in the specified directory.

**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.

**Syntax**

```
Appscan [/o <filename> /s <target directory> /x <extension strung /e /a /p /verbose /warnings /?] 
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file name</td>
<td>Output file name and path.</td>
</tr>
<tr>
<td>/o</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Application Control Policy**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s &lt;target directory&gt;</td>
<td>Specifies the directory, including all subdirectories, to scan.</td>
</tr>
<tr>
<td></td>
<td>• You must enclose the directory/path string in double quotes.</td>
</tr>
<tr>
<td></td>
<td>• If no directory is specified, the scan runs in the current directory only.</td>
</tr>
<tr>
<td>/x &lt;extension string&gt;</td>
<td>Specifies the file extension(s) to include in the scan.</td>
</tr>
<tr>
<td></td>
<td>• The extension string can include many extensions, each separated by a semi-colon.</td>
</tr>
<tr>
<td></td>
<td>• You must put a period before each file extension.</td>
</tr>
<tr>
<td></td>
<td>• You must enclose full extension string in double quotes.</td>
</tr>
<tr>
<td></td>
<td>• You must specify a target directory using the /s switch.</td>
</tr>
<tr>
<td></td>
<td>• If you do not use the /x parameter only .exe executable files are included in the scan</td>
</tr>
<tr>
<td>/e</td>
<td>Include all executable files in the specified directory regardless of the extension. Do not use /e together with /x.</td>
</tr>
<tr>
<td>/a</td>
<td>Includes additional file properties for each executable.</td>
</tr>
<tr>
<td>/p</td>
<td>Shows progress messages during the scan.</td>
</tr>
<tr>
<td>/verbose</td>
<td>Shows progress and error messages during the scan.</td>
</tr>
<tr>
<td>/warnings</td>
<td>Shows warning messages during the scan.</td>
</tr>
<tr>
<td>/? or /help</td>
<td>Shows the command syntax and help text.</td>
</tr>
</tbody>
</table>

**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 Appscan XML Files

After you generate the Appscan XML file, you import it to the Endpoint Security Management Server.

**Note** - You must remove all special characters, such as trademarks or copyright symbols, from the XML file before importing it.

**To import an Appscan XML file:**
1. In the **Policy** tab > **Application Control** rule, right click the **Allowed apps list** Action.
2. Select **Import Programs**.
3. In the **Import Programs** window, go to and select the applicable Appscan XML file.
4. Click **Import**.
   
   When applications included in the imported file are found on endpoint computers, they are automatically added to the **Allowed** or **Block** applications group.
Chapter 18

Client Settings Policy

In This Section:

Client Settings Policy Actions ................................................................. 145

In a large organization, creating a common policy for multiple clients eases deployment and reduces maintenance tasks.

Client Settings Policy Actions

The Client Settings Actions 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 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.

• Graphics that show in the Pre-boot and Onecheck Logon - For each of these graphics, you can use the default image or click Select to upload a new image:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Size of Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-boot Background Image</td>
<td>Image on Pre-boot screen behind the smaller logon window</td>
<td>800 x 600 pixels</td>
</tr>
<tr>
<td>Pre-boot Screen Saver</td>
<td>Image that shows when the system is idle</td>
<td>260 x 128 pixels</td>
</tr>
<tr>
<td>Pre-boot Banner Image</td>
<td>The banner image on the smaller logon window</td>
<td>447 x 98 pixels</td>
</tr>
<tr>
<td>OneCheck Logon Background Image</td>
<td>Image in the background of the Windows logon window if OneCheck Logon is enabled</td>
<td>256 KB or smaller</td>
</tr>
</tbody>
</table>
**Log Upload**

The default log upload Action is *Allow log upload to Endpoint Policy Servers.*

These Software Blades upload logs to the Endpoint Policy Server:
- Firewall
- Anti-Malware
- Compliance
- Full Disk Encryption
- Media Encryption & Port Protection
- Application Control

You can change these settings:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Log Upload</td>
<td>Select to enable log upload. Clear to disable log upload.</td>
</tr>
<tr>
<td>Log upload interval</td>
<td>Frequency in minutes between logged event uploads. (Default = 1 minute)</td>
</tr>
<tr>
<td>Minimum number of events before attempting an upload</td>
<td>Upload logged events to the server only after the specified number of events (default = 1)</td>
</tr>
<tr>
<td>Maximum number of events to upload</td>
<td>Maximum number of logged events to upload to the server (default = 1000)</td>
</tr>
<tr>
<td>Maximum age of event before upload</td>
<td>Optional: Upload only logged events that are older than the specified number of days (default=5 days)</td>
</tr>
<tr>
<td>Discard event if older than</td>
<td>Optional: Do not upload logged events if they are older than the specified number of days (default = 90 days)</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default reminder interval</td>
<td>Set the time, in minutes, after which users are reminded to install the client.</td>
</tr>
<tr>
<td>Force Installation and automatically restart after</td>
<td>Set the time, in hours, after which the installation starts automatically.</td>
</tr>
<tr>
<td>Client Uninstall Password</td>
<td>Set a password that the end user must enter before uninstalling the client.</td>
</tr>
<tr>
<td>Legacy Client Uninstall Password</td>
<td>Set a password that the end user must enter before uninstalling a legacy client.</td>
</tr>
</tbody>
</table>
**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 Software Blades:

- **Firewall**
- **Application Control**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to disable network protection on their computers</td>
<td>A Disable Network Protection option shows in the right-click menu of the client icon from the notification area.</td>
</tr>
<tr>
<td>Do not allow users to disable network protection on their computers</td>
<td>Only an administrator can disable a user's network protection.</td>
</tr>
</tbody>
</table>

**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 Software Blade:
   - **Allow Log** - To generate logs for events.
   - **Allow Alert** - To generate alerts for events.
Chapter 19

Access Zones Policy

In This Section:
- Trusted Zone ......................................................................................................... 148
- Changing the Access Zones Policy ...................................................................... 149
- Network Objects .................................................................................................... 150

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.

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 gateway address range
• Internet gateways
• Local subnets
• Security servers (for example, RADIUS, ACE, or TACACS 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.

Add and remove network objects from the Trusted Zone to change it.

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 Properties.
   The Properties 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. Select the Object Type.
4. Edit the Name and Description of the Zone.
5. Click OK.
6. 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 SmartDashboard. When you create a new object, it is also available in SmartDashboard. If you change an object in the SmartEndpoint or SmartDashboard, 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:

<table>
<thead>
<tr>
<th>Object Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the host you want to use as a network object.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>A description of the network object.</td>
</tr>
</tbody>
</table>

**Configuring an Address Range as a Network Object**

Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Object Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>First IP Address / Last IP Address</td>
<td>The first and last IP addresses for the network object.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>A description of the network object.</td>
</tr>
</tbody>
</table>
**Configuring a Network as a Network Object**

Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Object Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The network address you want to use as a network object.</td>
</tr>
<tr>
<td>Net Mask</td>
<td>The net mask.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>A description of the network object.</td>
</tr>
</tbody>
</table>

**Configuring a Site as a Network Object**

Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The full LDAP name of the host of the site you want to use as a network object. For example, hostname.acme.com.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network object.</td>
</tr>
</tbody>
</table>

**Configuring a Group as a Network Object**

1. Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network object.</td>
</tr>
</tbody>
</table>

2. Select from the **Available Objects** column, or create new objects.

**Configuring a Network Group With Exclusion**

Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
</tbody>
</table>
### Configuring a Site Group as a Network Object

1. Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network object.</td>
</tr>
</tbody>
</table>

2. Select an object from the **Available Objects** column, or create a new object of the type:
   - Site
   - Site Group
Chapter 20

Remote Access VPN

The Remote Access VPN Blade is a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel.

The Remote Access VPN client included in this release is **SmartEndpoint-managed Endpoint Security VPN E80.50**. For more information, see the E80.50 Endpoint Security and Remote Access VPN Clients homepage (http://supportcontent.checkpoint.com/solutions?id=sk92971).
Chapter 21

Remote Help

In This Section:

- Overview of Remote Help .................................................................................... 154
- Giving Remote Help to Full Disk Encryption Users .............................................. 154
- Media Encryption & Port Protection Remote Help Workflow ............................. 155
- Disabling Remote Help ......................................................................................... 156

Overview of 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 specified 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 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 for users who have forgotten their fixed passwords. For USB storage devices protected by Media Encryption & Port Protection policies, only remote password change is available.

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:

   - 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.
Remote Help

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:
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:
   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:

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.
Disabling and Deleting Rules • 131
Disabling Remote Help • 156
Disaster Recovery with High Availability • 74
Discovered Devices • 25
Disk Encryption • 84
Dynamic Mount Utility • 93

E
Editing Device Access Setting • 113
Editing Device Details • 111
Editing Properties of Non-AD Objects • 32
Enabling the Management Server to be an Endpoint Policy Server • 64
Endpoint Policy Server Proximity Analysis • 63
Endpoint Security Active Directory Authentication • 77
Endpoint Security Administrator Roles • 35
Endpoint Security Analysis Report • 21
Endpoint Security Analysis Report Action • 134
Endpoint Security Introduction • 9
Endpoint Security Licenses • 13
Endpoint Security Product Licenses • 13
Endpoint Security Services and Ports • 11
Enforcing Rules According to States • 58
Environments with Endpoint Security • 73
Exclude Files and Folders from Scan • 127
Exporting Packages • 42
External Endpoint Policy Servers • 61

F
Failover • 68
Finding Components in SmartEndpoint • 27
Firewall Policy • 129
Full Disk Encryption • 24
Full Disk Encryption Deployment Phase • 96
Full Disk Encryption Installation and Deployment • 90
Full Disk Encryption Logs • 96
Full Disk Encryption Policy • 84
Full Disk Encryption Recovery • 92
Full Disk Encryption Rule Actions • 84
Full Disk Encryption Troubleshooting • 94
Full Recovery with Recovery Media • 92

G
Getting and Applying Contracts • 15
Getting Licenses • 14
Getting the Initial Client Packages • 40
Giving Remote Help to Full Disk Encryption Users • 154
Global Automatic Access Action • 120
Global Pre-boot Authentication Settings • 99
Gradual Upgrade • 48

H
Hotspot Settings • 132
How do Endpoint Policy Servers Work? • 62
How Synchronization Works • 71
How to Back Up and Restore • 82

I
Important Information • 3
Importing Appscan XML Files • 143
Importing Program Rules • 142
Inbound Traffic Rules • 129
Inheritance and Rule Priority • 56
Initial Security Client Analysis • 46
Installing and Upgrade Settings • 146
Installing and Configuring an Endpoint Policy Server • 61
Installing Packages on Clients • 44
Installing Policy Changes on Clients • 59
Installing the Client Using the CLI • 45
IPv6 Traffic • 132

L
License Enforcement • 14
License Status • 16
Licenses Report • 26
Log Actions • 117
Log Upload • 146

M
Malware Signature Updates • 125
Malware Treatment • 128
Management High Availability • 67
Managing Computers • 31
Managing OUs or Groups • 30
Managing Users • 30
Managing Users and Computers • 28
Managing Users of a Computer • 31
Manual Synchronization with Endpoint Security • 73
Media Encryption & Port Protection • 25
Media Encryption & Port Protection Policy • 106
Media Encryption & Port Protection Remote Help Workflow • 155
Media Encryption & Port Protection Terminology • 106
Media Encryption Site Actions • 119
Media Lockout Settings • 116
Migrating from other Mac Products • 47
Monitoring Compliance States • 138
Monitoring Endpoint Policy Server Activity • 65
Monitoring Virtual Group Objects • 38

N
Network Objects • 149
Notes and Cautions - Windows • 47
Notes on Using Smart Cards • 104

O
Offline Access Actions • 114
Offline Upgrades • 49
OneCheck Logon • 89
OneCheck User Settings Policy • 98
OneCheck User Settings Policy Actions • 98
Online Upgrades • 50
Optional System Components • 11
Organization-Centric model • 12
Outbound Traffic Rules • 130
Overview of Backup and Restore • 82
Overview of Compliance • 133
Overview of Endpoint Policy Servers • 61
Overview of Endpoint Security Policy • 54
Overview of Full Disk Encryption • 84
Overview of Management High Availability • 67
Working with Policy Actions • 57
Working with Rules • 56
Working with Software Blade Packages • 41
Working with the Application Control Policy • 140
Working with Virtual Groups • 36