Important Information

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

**Check Point E80.65**
For more about this release, see the E80.65 home page [http://supportcontent.checkpoint.com/solutions?id=sk115512](http://supportcontent.checkpoint.com/solutions?id=sk115512).

**Latest Version of this Document**
To learn more, visit the Check Point Support Center [https://supportcenter.checkpoint.com](https://supportcenter.checkpoint.com).

**Feedback**
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments [mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security R77.30.03 Management Server Administration Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security R77.30.03 Management Server Administration Guide).
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 November 2018</td>
<td>Updated <em>Active Directory Scanner</em> (on page 39) and <em>Configuring a Directory Scanner Instance</em> (on page 40)</td>
</tr>
<tr>
<td></td>
<td>Changed &quot;all other servers&quot; to &quot;the Remote Help servers&quot; (on page 91)</td>
</tr>
<tr>
<td></td>
<td>Added links to SecureKnowledge articles for <em>Upgrading Full Disk Encryption</em> (on page 114), and added more <em>Client Requirements for Full Disk Encryption Deployment</em> (on page 113)</td>
</tr>
<tr>
<td></td>
<td>Updated <em>Changing the Access Zones Policy</em> (on page 221)</td>
</tr>
<tr>
<td>20 June 2017</td>
<td>Added <em>Anti-Ransomware Files</em> (on page 187)</td>
</tr>
<tr>
<td></td>
<td>Updated <em>SandBlast Environment Settings</em> (on page 204)</td>
</tr>
<tr>
<td></td>
<td>Added <em>Configuring Multiple SandBlast Appliances</em> (on page 205)</td>
</tr>
<tr>
<td>16 February 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>2</td>
</tr>
<tr>
<td>Endpoint Security Introduction</td>
<td>12</td>
</tr>
<tr>
<td>Overview of the System Architecture</td>
<td>12</td>
</tr>
<tr>
<td>Optional System Components</td>
<td>13</td>
</tr>
<tr>
<td>Endpoint Security Services and Ports</td>
<td>13</td>
</tr>
<tr>
<td>Centralized Organization of Users and Computers</td>
<td>14</td>
</tr>
<tr>
<td>Organization-Centric model</td>
<td>14</td>
</tr>
<tr>
<td>Policy-centric Model</td>
<td>15</td>
</tr>
<tr>
<td>Centralized Deployment</td>
<td>15</td>
</tr>
<tr>
<td>Centralized Monitoring</td>
<td>15</td>
</tr>
<tr>
<td>Endpoint Security Licenses</td>
<td>16</td>
</tr>
<tr>
<td>Endpoint Security Product Licenses</td>
<td>16</td>
</tr>
<tr>
<td>Demo and Temporary Licenses</td>
<td>17</td>
</tr>
<tr>
<td>License Enforcement</td>
<td>17</td>
</tr>
<tr>
<td>Getting Licenses</td>
<td>17</td>
</tr>
<tr>
<td>Getting and Applying Contracts</td>
<td>18</td>
</tr>
<tr>
<td>Configuring a Proxy for Internet Access</td>
<td>19</td>
</tr>
<tr>
<td>License Status</td>
<td>19</td>
</tr>
<tr>
<td>Using SmartEndpoint</td>
<td>20</td>
</tr>
<tr>
<td>Overview Tab</td>
<td>20</td>
</tr>
<tr>
<td>Policy Tab</td>
<td>21</td>
</tr>
<tr>
<td>Users and Computers Tab</td>
<td>21</td>
</tr>
<tr>
<td>Reporting Tab</td>
<td>22</td>
</tr>
<tr>
<td>Alerts</td>
<td>22</td>
</tr>
<tr>
<td>Push Operations</td>
<td>24</td>
</tr>
<tr>
<td>Compliance</td>
<td>26</td>
</tr>
<tr>
<td>Activity Reports</td>
<td>27</td>
</tr>
<tr>
<td>Software Deployment</td>
<td>27</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>28</td>
</tr>
<tr>
<td>User Authentication (OneCheck)</td>
<td>28</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>29</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>30</td>
</tr>
<tr>
<td>SandBlast Agent Anti-Bot</td>
<td>30</td>
</tr>
<tr>
<td>Licenses Report</td>
<td>30</td>
</tr>
<tr>
<td>Policy Reports</td>
<td>31</td>
</tr>
<tr>
<td>Deployment Tab</td>
<td>32</td>
</tr>
<tr>
<td>Client logging</td>
<td>32</td>
</tr>
<tr>
<td>Finding Components in SmartEndpoint</td>
<td>33</td>
</tr>
<tr>
<td>Show/Hide Blades</td>
<td>33</td>
</tr>
<tr>
<td>Users and Computers</td>
<td>34</td>
</tr>
<tr>
<td>Managing Users and Computers</td>
<td>34</td>
</tr>
<tr>
<td>Using the Users and Computers Tab</td>
<td>34</td>
</tr>
<tr>
<td>Using the Object Details Window</td>
<td>34</td>
</tr>
<tr>
<td>Using the Users and Computers Tree</td>
<td>35</td>
</tr>
<tr>
<td>Managing Users</td>
<td>36</td>
</tr>
<tr>
<td>Managing OUs or Groups</td>
<td>37</td>
</tr>
<tr>
<td>Managing Computers</td>
<td>37</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Protection for Servers</td>
<td>67</td>
</tr>
<tr>
<td>Working with Rules</td>
<td>68</td>
</tr>
<tr>
<td>Inheritance and Rule Priority</td>
<td>68</td>
</tr>
<tr>
<td>Creating New Policy Rules</td>
<td>69</td>
</tr>
<tr>
<td>Working with Policy Actions</td>
<td>69</td>
</tr>
<tr>
<td>Policy Toolbar</td>
<td>70</td>
</tr>
<tr>
<td>Enforcing Rules According to States</td>
<td>71</td>
</tr>
<tr>
<td>Installing Policy Changes on Clients</td>
<td>71</td>
</tr>
<tr>
<td>The Heartbeat Interval</td>
<td>72</td>
</tr>
<tr>
<td>Configuring the “About to be Restricted” State</td>
<td>72</td>
</tr>
<tr>
<td>External Endpoint Policy Servers</td>
<td>74</td>
</tr>
<tr>
<td>Overview of Endpoint Policy Servers</td>
<td>74</td>
</tr>
<tr>
<td>Installing and Configuring an Endpoint Policy Server</td>
<td>74</td>
</tr>
<tr>
<td>Endpoint Policy Server Configuration</td>
<td>74</td>
</tr>
<tr>
<td>How do Endpoint Policy Servers Work?</td>
<td>75</td>
</tr>
<tr>
<td>Configuring Policy Server Settings</td>
<td>76</td>
</tr>
<tr>
<td>Endpoint Policy Server Proximity Analysis</td>
<td>76</td>
</tr>
<tr>
<td>Enabling the Management Server to be an Endpoint Policy Server</td>
<td>77</td>
</tr>
<tr>
<td>Policy Server and Management Server Communication</td>
<td>78</td>
</tr>
<tr>
<td>Monitoring Endpoint Policy Server Activity</td>
<td>79</td>
</tr>
<tr>
<td>Management High Availability</td>
<td>80</td>
</tr>
<tr>
<td>Overview of Management High Availability</td>
<td>80</td>
</tr>
<tr>
<td>The High Availability Environment</td>
<td>80</td>
</tr>
<tr>
<td>Planning for Management High Availability</td>
<td>81</td>
</tr>
<tr>
<td>Configuring a Secondary Server in SmartDashboard</td>
<td>81</td>
</tr>
<tr>
<td>Failover</td>
<td>82</td>
</tr>
<tr>
<td>Changing a Server to Active or Standby</td>
<td>82</td>
</tr>
<tr>
<td>Understanding Server Status</td>
<td>83</td>
</tr>
<tr>
<td>Before Failover</td>
<td>83</td>
</tr>
<tr>
<td>Synchronizing Active and Standby Servers</td>
<td>84</td>
</tr>
<tr>
<td>Synchronization Procedures</td>
<td>84</td>
</tr>
<tr>
<td>Manual Synchronization with Endpoint Security</td>
<td>85</td>
</tr>
<tr>
<td>Which Data is Synchronized</td>
<td>85</td>
</tr>
<tr>
<td>How Synchronization Works</td>
<td>86</td>
</tr>
<tr>
<td>Online Automatic Sync</td>
<td>86</td>
</tr>
<tr>
<td>Running Migrate in Online Synchronization Environment</td>
<td>87</td>
</tr>
<tr>
<td>Synchronization Status</td>
<td>88</td>
</tr>
<tr>
<td>Synchronization Troubleshooting</td>
<td>88</td>
</tr>
<tr>
<td>Environments with Endpoint Security</td>
<td>89</td>
</tr>
<tr>
<td>Synchronizing MSI Files and Drivers</td>
<td>89</td>
</tr>
<tr>
<td>Updating the PAT Version on the Server</td>
<td>90</td>
</tr>
<tr>
<td>Deleting a Server</td>
<td>90</td>
</tr>
<tr>
<td>Synchronization with Endpoint Security</td>
<td>90</td>
</tr>
<tr>
<td>Disaster Recovery with High Availability</td>
<td>91</td>
</tr>
<tr>
<td>Recovery by Promoting a Secondary Server</td>
<td>91</td>
</tr>
<tr>
<td>Promoting a Secondary Server to Primary</td>
<td>91</td>
</tr>
<tr>
<td>Active Directory Authentication</td>
<td>93</td>
</tr>
<tr>
<td>Endpoint Security Active Directory Authentication</td>
<td>93</td>
</tr>
<tr>
<td>Configuring Authentication</td>
<td>94</td>
</tr>
<tr>
<td>Configuring Active Directory for Authentication</td>
<td>94</td>
</tr>
<tr>
<td>Configuring Global Authentication</td>
<td>95</td>
</tr>
</tbody>
</table>
Strengthening the LDAP Communication ................................................................. 96
Troubleshooting Authentication in Server Logs....................................................... 98
Troubleshooting Authentication in Client Logs....................................................... 99
Server and Client Communication ........................................................................... 100
Overview of Server and Client Communication .................................................. 100
SHA-256 Certificate Support ....................................................................................... 100
TLSv1.2 Support ........................................................................................................... 101
Backup and Restore ..................................................................................................... 102
Overview of Backup and Restore .............................................................................. 102
Prerequisites ................................................................................................................ 102
How to Back Up and Restore ..................................................................................... 102
Updating the PAT Version on the Server after Restore ............................................. 103
Full Disk Encryption .................................................................................................... 104
Overview of Full Disk Encryption ............................................................................. 104
Configuring Full Disk Encryption Policy Rules ....................................................... 104
Disk Encryption ............................................................................................................ 104
Authentication before Operating System (Pre-boot) ................................................. 106
User Authorization before Encryption ....................................................................... 111
OneCheck Logon ......................................................................................................... 112
Full Disk Encryption Installation and Deployment .................................................... 113
Client Requirements for Full Disk Encryption Deployment ....................................... 113
Upgrading Full Disk Encryption .................................................................................. 114
Completing Full Disk Encryption Deployment on a Client ......................................... 114
Stages of the Deployment Phase ................................................................................ 114
Primary Full Disk Encryption Components .............................................................. 115
Full Disk Encryption Recovery .................................................................................... 115
Full Recovery with Recovery Media .......................................................................... 115
Using Drive Slaving Utility ......................................................................................... 117
Dynamic Mount Utility ............................................................................................... 118
Full Disk Encryption Self-Help Portal ....................................................................... 118
Activating the Self-Help Portal .................................................................................. 119
Configuring the Self-Help Portal ................................................................................. 119
User Settings for the Self-Help Portal ....................................................................... 120
Monitoring the Self-Help Portal Policy ..................................................................... 120
Full Disk Encryption Troubleshooting ...................................................................... 120
Using CPinfo ............................................................................................................... 120
Using CPinfoPreboot ................................................................................................. 121
Pre-boot Issues ........................................................................................................... 122
Full Disk Encryption Logs ......................................................................................... 123
Upgrade Issues ............................................................................................................ 123
Full Disk Encryption Deployment Phase ...................................................................... 123
OneCheck User Settings .......................................................................................... 125
Overview of OneCheck User Settings ...................................................................... 125
Configuring OneCheck User Settings Policy Rules ................................................ 125
Pre-boot Authentication Methods .......................................................................... 125
Password Complexity and Security ........................................................................... 128
Password Synchronization ......................................................................................... 129
Account Lock ............................................................................................................... 129
Logon Settings ............................................................................................................. 130
Remote Help Permissions ............................................................................................ 131
Managing Authorized Pre-boot Users and Nodes ...................................................... 132
Endpoint Security Introduction

In This Section:

- Overview of the System Architecture ................................................................. 12
- Endpoint Security Services and Ports ................................................................. 13
- Centralized Organization of Users and Computers ............................................. 14
- Centralized Deployment ..................................................................................... 15
- Centralized Monitoring ..................................................................................... 15

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartEndpoint</td>
<td>Check Point SmartConsole application to deploy, monitor and configure Endpoint Security clients and policies. Install on the <strong>Endpoint Security Management Server</strong> or on a computer that supports the client installation.</td>
</tr>
<tr>
<td>Endpoint Security Management Server</td>
<td>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.</td>
</tr>
<tr>
<td>Endpoint Security Blades</td>
<td>Software blades available on the Endpoint Security Management Server. You can install any or all of these blades on endpoint clients. See Software Blades [on page 66].</td>
</tr>
</tbody>
</table>
Endpoint Security Introduction

<table>
<thead>
<tr>
<th>Endpoint Security Database</th>
<th>Holds policies that enforce security on endpoint clients, holds user and computer objects, licensing, and Endpoint monitoring data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Scanner</td>
<td>Software component that synchronizes the structure and contents of the Active Directory with the Endpoint Security policy database.</td>
</tr>
</tbody>
</table>

### Endpoint Security Clients

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security Clients</td>
<td>Application installed on end-user computers to monitor security status and enforce security policies.</td>
</tr>
<tr>
<td>Endpoint Agent</td>
<td>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)</td>
</tr>
<tr>
<td>Endpoint Security Blades</td>
<td>Software blades deployed on the endpoint client.</td>
</tr>
</tbody>
</table>

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

### 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</td>
<td>TCP/80</td>
<td>Heartbeat, communicates policy, status and compliance changes.</td>
</tr>
<tr>
<td>• Heartbeat</td>
<td>ESP</td>
<td>TCP/80</td>
<td></td>
</tr>
<tr>
<td>• Log upload</td>
<td>ESP</td>
<td>TCP/80</td>
<td></td>
</tr>
<tr>
<td>• Full Disk Encryption Recovery Data Upload</td>
<td>ESP</td>
<td>TCP/443</td>
<td></td>
</tr>
<tr>
<td>• Media Encryption &amp; Port Protection Key Exchange</td>
<td>ESP</td>
<td>TCP/443</td>
<td></td>
</tr>
<tr>
<td>• Full Disk Encryption User Acquisition &amp; User credentials.</td>
<td>ESP</td>
<td>TCP/443</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>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Secure Internal Communication</td>
<td>SIC</td>
<td>TCP/18190 - 18193</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 predefined security policies before setting up the organization. The Endpoint Security Management server interface provides a granular view of all the Endpoint Security policies, grouped by the 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 blades 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

The 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.
Endpoint Security Licenses

In This Section:

- Endpoint Security Product Licenses ................................................................. 16
- Demo and Temporary Licenses ................................................................. 17
- License Enforcement .............................................................................. 17
- Getting Licenses ......................................................................................... 17
- Getting and Applying Contracts ......................................................... 18
- License Status ......................................................................................... 19

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>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</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This license automatically comes with the Container License</td>
</tr>
<tr>
<td></td>
<td>• URL Filtering</td>
</tr>
<tr>
<td></td>
<td>• Anti-Bot</td>
</tr>
<tr>
<td></td>
<td>• Forensics and Anti-Ransomware</td>
</tr>
<tr>
<td></td>
<td>• Capsule Docs</td>
</tr>
<tr>
<td></td>
<td>• Threat Emulation</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](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 (on page 18).

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.
   a) Make sure that Version is R80 and above.
   b) 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:
   a) SmartUpdate
   b) The Gaia or SecurePlatform WebUI.
   c) The cplic CLI command
   d) 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_CNTRCTMNGR.xml`
2. Change the `<interval>` value as necessary.
3. Run cpstop and cpstart.

To apply a contract manually:

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 in SmartDashboard.

To configure a proxy for the Endpoint Security Management Server:
1. In SmartDashboard, open the Endpoint Security Management Server object.
2. Select Topology > Proxy.
3. Select Use custom proxy settings for this network object.
4. Enter the URL and port.
5. Click OK.

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
Using SmartEndpoint

In This Section:

Overview Tab ................................................................................................................. 20
Policy Tab ...................................................................................................................... 21
Users and Computers Tab ........................................................................................... 21
Reporting Tab................................................................................................................ 22
Deployment Tab ............................................................................................................ 32
Client logging ................................................................................................................ 32
Finding Components in SmartEndpoint ................................................................. 33
Show/Hide Blades ......................................................................................................... 33

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 (on page 22) in Reporting tab > Alerts.

Security Status

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

• Deployment Progress - Shows the progress of package deployment to endpoint computers.
• Blade Health Check - Shows which computers have installed Blades that are not running.
Using SmartEndpoint

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

For each category you can see:
- **Trend** tab - A line chart that shows the trend over time.
- **Endpoints** tab - A table that shows Endpoint computers in greater detail.

You can also click the **Getting Started** link to run the **Endpoint Security Express Setup Wizard**. Do the steps in the wizard pages to quickly configure the default policy for each Blade. The wizard also lets you run the Directory Scanner (on page 39) and configure Deployment rules (on page 52).

**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 **OK**.
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 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 Area - Icons and Controls

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search</strong></td>
<td>Enter a text string to search all columns and results that contain the string are shown.</td>
</tr>
<tr>
<td><strong>Status:</strong></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><strong>In:</strong></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>📅</td>
<td>Click to see other options available. Options include Push Operations (on page 24). Some options are not available for all reports.</td>
</tr>
<tr>
<td><strong>Add to virtual group</strong></td>
<td>Add the selected objects to a virtual group.</td>
</tr>
<tr>
<td><strong>Toggle chart percentage</strong></td>
<td>Add and remove the percentages shown on the graph.</td>
</tr>
<tr>
<td><strong>Hide Chart/Show Chart</strong></td>
<td>Close or open the pane with the graph.</td>
</tr>
<tr>
<td><strong>Export Report</strong></td>
<td>Export the report results to an XLS, HTML, or CSV file.</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:

- Certificate Expiration
- Compliance Warning
- Deployment Failed
- Encryption Problem
Anti-Malware Issues

The lower section of the pane contains two tabs:

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

**Configuring Alert Messages**

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

<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 an Email Server

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

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

Troubleshooting issues with email settings

If the email server does not send alerts and email server authentication is not necessary do these steps:
1. In SmartEndpoint, select Manage > Email Server Settings > Configure Settings.
2. In the Email Server Settings window select User authentication is required.
   Configure these parameters:
   - Port - Leave the default (25).
   - User Name - Enter a fictitious email address. This address will show as the sender of email alerts.
   - Password - Enter a fictitious password. This is not used.
3. Optional: Trigger an alert to test the email server.

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.

• **SandBlast Agent Forensics Remediation and Anti-Ransomware**
  - **Analyze by URL** - Manually trigger incident analysis. Enter a URL to inspect and, optionally, search for an incident related to the URL.
  - **Analyze by Process or File** - Manually trigger incident analysis. Enter the full path to the file and, optionally, search for an incident related to the process or file.

• **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 an object (user or computer) and select a blade, and then 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 a blade and 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.
    Optional: Select **Inform user** and click **Configure** to configure a notification message that users see and in how many minutes the operation will occur. If you do not select **Inform user**, the operation runs silently.
  - **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 181) 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 (on page 72).
- **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

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

This group includes these reports:

- **Full Disk Encryption Versions** - Shows the installed version of the Full Disk Encryption 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 which endpoints use Check Point Anti-Malware and which use a third-party Anti-Virus provider.
- **Anti-Malware Scanned Date** - Shows status by the last scan date
- **Anti-Malware Updated On** - Shows computers that have Anti-Malware updates installed

**SandBlast Agent Anti-Bot**

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

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

**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*. 
Policy Reports

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

To enable scheduled Policy Reports:

1. On the Endpoint Security Management Server, run: `cpstop`
2. Open the server’s `local.properties` file:
   `$UEPMDIR/engine/conf/local.properties`
3. Find the line: `#emon.scheduler.time=9:55:00,10:55:00,15:33:00`
   - Delete the `#` from the line
   - Edit the times to show the hour when the reports will be created. Reports will be created each day at these times.
   - Make sure the line is in this format:
     `emon.scheduler.time=HH:mm:ss,HH:mm:ss,HH:mm:ss`
     with no spaces between the times and commas.
4. Find the line: `#emon.scheduler.max.reports=10`
   - Delete the `#` from the line
   - The number represents the maximum number of reports that can remain in the report directory. The oldest ones are overridden by newer ones. Optional: Edit the number.
   - Make sure the line is in this format: `emon.scheduler.max.reports=<number of reports to save>`.
5. Find the line: `#emon.scheduler.policyreport=true`
   - Delete the `#` from the line
   - Make sure the line is in this format: `emon.scheduler.policyreport=true`
6. Create a new folder in `$FWDIR/conf/SMC_Files/uepm/reports/`. Run:
   `mkdir $FWDIR/conf/SMC_Files/uepm/reports`
   `chmod 2777 $FWDIR/conf/SMC_Files/uepm/reports`
   The name of the report will be: `policyReport<number>.csv`
   The number represents the creation time so newer reports have higher numbers.
7. Run: `cpstart`

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

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

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

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

Endpoint Security clients upload logs to the Endpoint Security Management Server.
On the server, the logs are stored in the common log database, which is read by SmartLog or SmartView Tracker.

Note - The Remote Access 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
### Logs File

<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, epslog1.log is deleted. Can be viewed with any ASCII viewer, or by using the client viewer, or by manually running: C:\Program Files\Common Files\Check Point\Logviewer\EPS_LogViewer.exe</td>
</tr>
<tr>
<td>epslog.ini</td>
<td>Internal files, compressed and encrypted.</td>
</tr>
<tr>
<td>epslog.1.elog</td>
<td></td>
</tr>
<tr>
<td>epslog.1.elog.hmac</td>
<td></td>
</tr>
</tbody>
</table>

Logs are 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.

See the [E80.65 Client User Guide](http://supportcontent.checkpoint.com/solutions?id=sk115512) for more details.

### 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.

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**.
Users and Computers

In This Section:

Managing Users and Computers ................................................................. 34
Active Directory Scanner ............................................................................. 39
Endpoint Security Administrator Roles ....................................................... 43
Working with Virtual Groups ...................................................................... 43

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.
- **Global Actions** - From here you can perform different SmartEndpoint operations.
- **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 [on page 22] 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 (on page 22) are shown.

**Changing Authentication Settings**

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

- The Pre-boot authentication method (on page 125) when the Full Disk Encryption Blade is active. The default authentication method is **Password**.
- Lock a user out (on page 129) 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.
- **External Users** - For the Capsule Docs blade, add users from outside of the organization who can open documents in the Capsule Docs Viewer or Editor. Permissions for these users are defined in the Capsule Docs Policy rules.

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 (on page 38) - 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, Pre-boot, and Remote Help.

• OneCheck User Settings - Opens a list of operations related to OneCheck User Settings, Pre-boot, and the Full Disk Encryption Self-Help Portal (on page 118).

• Anti-Malware - Opens a list of Push Operations related to Anti-Malware, Client Settings, and SandBlast Agent Forensics and Remediation. See Push Operations (on page 24).

• SandBlast Agent Forensics and Remediation - Opens a list of Push Operations related to SandBlast Agent Forensics and Remediation. See Push Operations (on page 24).

• Client Settings - Opens a list of Push Operations related to Client Settings. See Push Operations (on page 24).

• Address Range - Define a new address range.

• Capsule Docs - Opens a list of operations related to Capsule Docs and external users.

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 (on page 34) 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 (on page 34) 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.

Required Permissions to Active Directory

For the scan to succeed, the user account related to each Directory Scanner instance requires full read permissions to:
- The Active Directory root.
- All child containers and objects.
- The deleted objects container.

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

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

Required Configuration for Domains

On the Active Directory server, set the Groups Scope to Domain Local only.
Configuring a Directory Scanner Instance

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

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

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

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

If the domains use DNS servers, make sure that:

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

To create a scanner instance:

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

7. Click **OK**.

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

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

### The Organization Scanners Page

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

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

### Directory Synchronization

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

- New Active Directory objects are added to Endpoint Security and inherit a policy according to the Endpoint Security policy assignment.

- Deleted users are removed from the **Users and Computers** tree, but only if they had no encrypted removable media devices. Deleted users with encrypted removable media devices move to the **Deleted Users/Computers** folder. The user no longer exists in the Active Directory, but the server keeps the encryption keys for possible recovery. You can delete these users manually using SmartEndpoint.

- Computers deleted from the Active Directory that do not have Endpoint Security are deleted from **Users and Computers**.

- Computers deleted from the Active Directory that do have Endpoint Security move to the **Deleted Users/Computers** folder because they might require recovery. You can delete these computers manually from the Management Console.

- Objects updated in the Active Directory are also updated on the server.

- Unchanged records stay unchanged.
## Troubleshooting the Directory Scanner

<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 required read permissions to the Active Directory or to the deleted objects container.</td>
<td>Supply the required permissions.</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 read permission to that object. If the corrupt object is a container 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.


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 for 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 Groups

There are two types of virtual groups:

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

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

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**
• **Capsule Docs external users** - Contains users that have external permissions for Capsule Docs

• **Capsule Docs internal users** - Contains users that have external permissions for Capsule Docs

If you add objects to a virtual group with an installation package (on page 46), 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.
Deploying Endpoint Security Clients

In This Section:

Automatic Deployment Overview ................................................................. 47
Working with Software Blade Packages for Export ................................... 51
Software Blade Packages ........................................................................... 52
Advanced Package Settings ........................................................................ 53
Local Deployment Options ......................................................................... 54
Installing the Client Using the CLI .............................................................. 55
Seeing the Deployment Status .................................................................... 56
Initial Security Client Analysis ................................................................... 56
Deploying Mac Clients ............................................................................... 57
Upgrading Endpoint Security Clients ......................................................... 58
Upgrading Legacy Clients .......................................................................... 59
Troubleshooting the Installation ................................................................. 63
Uninstalling the Client on Windows ........................................................... 64
Configuring Log Forwarding ...................................................................... 64

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 (on page 47).
  - **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 (on page 51).

- For clients on Mac, see Deploying Mac Clients (on page 57).

Automatic Deployment Overview

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

1. **Initial Client** - This package includes the Endpoint Agent that communicates with the Endpoint Security Management Server. This must be distributed manually through an exported package.

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

For manual deployment and upgrades, install the **Software Blade Package**. Do not install the Initial Client first.
You can configure the policies for the Software Blades before or after you deploy the Software Blade package.

⚠️ **Important** - The name of client packages must stay **EPS.msi**.

### Deploying the Initial Client

You can get the Initial Client from SmartEndpoint, the distribution media, or download a E80.65 Endpoint Security client from the Support Center. If you do not get the Initial Client from SmartEndpoint, you must give endpoint users the Endpoint Security Management Server host name or IP address. They enter this information to connect to the Endpoint Security Management Server manually.

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

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

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

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

### 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**.
   The **Package download configuration** window opens.
3. Optional: To add users who install this package to a Virtual Group, click the arrow to expand **Virtual Group**.
   - Select **Select Virtual Group**. Endpoints installed with the exported package will automatically be added to it.
   - Select a Virtual Group or click **Add New** to create a new group.
4. For upgrades from R73: Click the arrow to expand **R73 Client Upgrade**.
   a) Select **Support R73 client upgrade**.
   b) Optional: To upgrade without user input, select **Silent Upgrade**. If this is not selected, users are prompted to upgrade.
   c) Optional: To force reboot after a silent upgrade, select **Force reboot**. If this is not selected, users are asked to reboot.
   d) Enter Legacy upgrade passwords if relevant for **Secure Access** and **Full Disk Encryption EW**.
5. Click **Download**.
6. In the Save Location, right-click and select **New > Folder**. Give the folder a name that describes the package contents, such as **Initial Client**.
7. Click **OK**.
The Endpoint Security Management Server downloads the package from the internet and saves it to the specified folder.

To get the Initial Client from the Support Center:
1. Create a folder for the Initial Client on your local computer.
4. In the Version filter section, select E80.65.
5. Download Endpoint Security E80.65 Client for Windows.
6. Create a new folder with a name that describes the package contents, such as ‘Initial Client.’
7. Copy EPS.msi to the folder.

Deploying the Software Blade Package with Deployment Rules
Software Deployment rules let you manage Software Blade 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 computers
- Specified Endpoint Security Virtual Groups, such as the predefined Virtual Groups ("All Laptops", "All Desktops", and others.). You can also define your own Virtual Groups.

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

Creating New Deployment Rules
To create new rules for automatic Software Deployment:
1. Click the Deployment tab and select Software Deployment Rules.
2. Click the Create Rule icon.
   The Create Rule Wizard opens.
3. In the Select Entities window, select an entity (OU, Virtual Group, or Computer). Double-click the node to show the items contained in that node.
4. Click Next.
5. In the Change Rule Action Settings window:
   - Select a package version or click Manage Client Versions to upload a different client version from in the Packages Repository.
   - Select Software Blades to install and clear Software Blades that are not to be installed with this rule.
6. Click Next.
7. In the Name and Comment window, enter a unique name for this rule and an optional comment.
8. Click Finish to add the rule to the Software Deployment Rules.
9. Click Save.
10. Install the policy.

Changing Existing Deployment Rules

To edit rules for automatic Software Deployment:

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

Installing Packages on Clients with Software Deployment

After the Initial Client is successfully deployed and you have Software Deployment rules, install Software Blade Packages easily from SmartEndpoint.

Edit the Client Settings rules to change client installation settings.

To install Software Blade Packages on endpoint computers:

1. On the Deployment tab, click Install.
2. If prompted, click Save to save the rules.
3. Select the Rules to install and then click Install.

To make sure that a rule does not install:

Right-click in the Actions column of a Software Deployment rule and select Do not install.
Working with Software Blade Packages for Export

You can deploy an exported Software Blade Package to endpoint clients with third-party deployment software. When you create a Software Blade Package for export, the Initial Client is usually included in the package, and not installed first.

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 Software Blade package for export:

1. In the Deployment tab, select Packages for Export.
2. To add a new package, click Add Package.
   The new package shows at the bottom of the list.
3. Double-click the Name cell in the applicable package and enter a package name.
4. Optional: Double-click the Version cell and select a different Endpoint Client version from the list.
   You can select Manage Client Versions, to add more package versions to the repository.
5. Click the Desktop Blades and Laptop Blades cells and then select the Software Blades to include in each package.
6. Optional: In the Settings column select a Virtual Group or create a new one. Users who install this package will automatically be put in this Virtual Group.
7. Optional: In the Settings column, if you defined 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
8. If you are upgrading legacy Endpoint Security release, in the Settings column:
   - Double-click the legacy upgrade option and select Support client pre-install upgrade.
   - Select Silent mode active or Silent mode not active.
   - Select the Legacy Secure Access option and click Configure Upgrade Password to enter and confirm the password.
   - Select the Legacy Full Disk Encryption EW option and click Configure Upgrade Password to enter and confirm the applicable passwords.
9. In the Software Deployment Rules window, click Save.

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

Defining the Default VPN Site

When you use an exported package, 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.

You cannot configure a default VPN site with automatic Software Deployment. To distribute a defined VPN site with Software Deployment, you can:

- Use Software Deployment to distribute a Software Blade Package without Remote Access VPN.
• Create a package for export that includes only Remote Access VPN and distribute it manually.

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 **Actions** column > **Selected blades**.
2. Select **Advanced Package Settings > VPN Client Settings** from the navigation tree.
3. Click **New** to create a new site or **Edit** to change the details of a site. Enter:
   - **Display name** - The name users see when they connect to the VPN.
   - **Site address** - The IP address of the site.
   - **Authentication method** - How users authenticate to the VPN. Make sure that users have all required information and hardware, if required.
      
This line can contain the **No VPN site defined** item or a predefined VPN site.
4. In the **Software Deployment Rules** window, click **Save**.

**Exporting Packages**

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

1. In the **Packages for Export** window, select a package.
2. Click **Download Package**.
3. In the **Export Package** window:
   a) Select the platform versions (32/64 bit) to export for laptops and desktops.
   b) Click **Download**.
4. Click **OK**.
5. Select a location to save the files.
   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.
6. 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.

**Software Blade Packages**

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. 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>
</tbody>
</table>
### 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
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
   - **SecurID KeyFob** - Endpoint users authenticate using a KeyFob hard token
   - **SecurID PinPad** - Endpoint users authenticate using the an SDTID token file and PIN
   - **Challenge-response** - Endpoint users authenticate using an administrator supplied response string in response to the challenge prompt.
5. Click **OK**.

---

<table>
<thead>
<tr>
<th>Directory Name</th>
<th>Contains These Client Packages</th>
</tr>
</thead>
<tbody>
<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>Master_SBA</td>
<td>32 bit SandBlast Agent blades with Firewall, Compliance, and Application Control</td>
</tr>
<tr>
<td>Master_SBA_x64</td>
<td>64 bit SandBlast Agent blades with Firewall, Compliance, and Application Control</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 directory is: $FWDIR/conf/SMC_Files/uepm/msi
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. In a Software Deployment rule, in the Actions column, click Endpoint Client Version and select Manage Client Versions.
2. Click an option:
   • Load the latest supported client version from the internet - Downloads the most recent file from Check Point servers.
   • Load a folder containing client installers - Select a folder that contains MSI packages from your network.
   • Load client installer file - Select a single MSI file to upload
   • Delete package - Select a package to delete and click this. Select Save. If a package is in use, a message shows that you cannot delete it.

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.

Local Deployment Options

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

To set up such a deployment, you must:
• Upload the packages to the Endpoint Security Management Server.
• Create a Software Deployment rule with the package version selected.
• Configure a Common Client Settings rule to allow deployment from local paths or URLs.
• Upload the packages to the defined local storage paths or URLs.

This is only supported on Windows clients.

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

To enable Software Deployment with a locally stored package:

2. Put the same packages in local storage location on client computers, for example C:\TEMP\EPS\32bit\EPS.msi.
3. Go to the **Policy** tab of SmartEndpoint > **Client Settings** rule.
4. In the Deployment Locations action, select **Enable deployments from local paths or URLs**. You can also **Clone the action**.
5. Double-click the action. The **Deployment Locations** window opens.
6. Make sure that **Allow to install software deployment packages from...** is selected.
7. Optional: Select **Enable Deployment from Server when no MSI was found in local paths or URLs**. When selected, if no MSI file is in the local paths or URLs, the client checks the Endpoint Security Management Server for packages.
8. Click **Add item** and select the **Package Location** to add paths for packages located on client computers. Select if each package is for 32 bit or 64 bit computers.
9. Click **OK**.
10. In the **Deployment** tab, create or edit a Software Deployment rule to use the package **Version** and assign it to computers.
11. Click **Save**.
12. Install Policy to deploy the rule to clients.

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

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

### 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</td>
<td>Do a fresh installation of the exported package</td>
</tr>
<tr>
<td>msiexec.exe /i EPS.msi REINSTALL=ALL</td>
<td>Reinstall all installed blades using the exported package</td>
</tr>
<tr>
<td></td>
<td></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 /qb! REINSTALL=DUMMY REINSTALLMODE=vomus</td>
<td>Add or remove blades using the exported package</td>
</tr>
<tr>
<td>msiexec /i EPS.msi</td>
<td>Upgrade using the specified exported package. This package must include the same blades that are presently installed.</td>
</tr>
</tbody>
</table>

You can add a parameter to enable the Fast Initial Encryption mode, for encryption of only Used Space (not Free Space) on the disk. See sk102026 http://supportcontent.checkpoint.com/solutions?id=sk102026 for details.

Logging Options
To create logs, do one of the following steps:
- Add /l*v <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>Logging</td>
</tr>
<tr>
<td>Reg_SZ</td>
<td>voicewarmup</td>
</tr>
</tbody>
</table>

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

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.

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.
2. In the window that opens, select which blades to include in the package and click Download.
   If more than one version is in the Package repository, select a client to download.
3. Optional: If Remote Access VPN is part of the package, you can configure a VPN site.
4. Select the location to save the package.
   The package starts to download.
5. The package, Endpoint_Security Installer.zip shows in the configured location. This is the file that you distribute to endpoint users.

To distribute the Mac client package:

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

To install the Mac client package on client computers:

1. Double-click the ZIP file to expand it.
2. Click the APP file that shows next to the zip file.
   The Check Point Endpoint Security Installer opens.
3. Click Install.
4. Enter a Name and Password to authorize the installation.
5. Click OK.
   Wait while package installs.
6. A message shows that the package installed successfully or failed for a specified reason. Click Close.
   If the installation was successful, the Endpoint Security icon shows in the menu bar.

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"
   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.

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 58.

- For Full Disk Encryption, see Upgrading Legacy Full Disk Encryption on page 61.
- If you install the Mac client on a computer that had E75 Endpoint Security VPN for Mac, it upgrades to E80.65 with its configuration settings preserved.

Upgrading Endpoint Security Clients

This section includes procedure for upgrading endpoint clients:

You can upgrade to E80.x clients from earlier versions of 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 E80) VPN clients, remove all Firewall related blades. Do this before the upgrade.
2. Make sure that the clients are connected to an Endpoint Security Management Server of the higher version.
3. Get a complete package with Initial Client and the Software Blade Package. Get this from the Software Deployment tab in one of these ways:
   - Download a package from the Packages for Export window.
   - In the Software Deployment Rules window, right-click in a rule and select Download Package. This includes the Initial Client and Software Blade Package.
4. Deploy the package.

Upgrading with Deployment Rules

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

To upgrade clients with 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, go to **Packages for Export**.
2. Select a package and click **Upgrade Profile**.
   A message opens that shows if an update is available.
3. Click **Yes** to confirm that you want to upgrade the profile.
4. In the **Export Package** window:
   a) Select the platform versions (32/64 bit) to export for laptops and desktops.
   b) Enter or browse to a destination folder.
5. 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.
6. 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** for the supported upgrade paths for this version. Legacy clients are those earlier than version E80. You must enter password information to upgrade legacy Secure Access and Full Disk Encryption.
Offline Upgrades

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

- All the passwords necessary to successfully uninstall legacy products
- The new client with the necessary 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 the Deployment tab, select Packages for Export from the tree.
2. Click Add.
   A new package shows in the list.
3. Optional: Change the package Name and Version.
4. In the Settings column, select Support client preinstall upgrade.
5. Under Support client preinstall upgrade, make these selections as necessary:
   a) Silent Mode - Choose if silent mode is active. When active, the procedure tool runs silently without user intervention. If silent mode is not active, users can see the GUI of the Upgrade tool. If silent mode is active, select what happens after the upgrade:
      - Force restart after upgrade.
      - Prompt user to restart after upgrade.
   b) Secure Access upgrade - To enable a Secure Access upgrade you must enter the uninstallation password. Click on Legacy Secure Access upgrade not supported and select Configure Upgrade Password.
      In the Legacy Secure Access Upgrade window, select Support Legacy upgrade and enter and confirm the uninstallation password.
   c) Legacy Full Disk Encryption upgrade - To enable an upgrade from legacy Full Disk Encryption EW, you must enter the uninstallation password. Click on Legacy Full Disk Encryption EW upgrade not supported and select Configure Upgrade Password.
      In the Legacy Full Disk Encryption EW window, select Support Legacy upgrade and enter and confirm the uninstallation password.
6. Make sure the 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:
    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.
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 58).

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.
- 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 (on page 58).
- 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 (on page 58).

**What effect does an upgrade have on users?**

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

**Do not:**

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

Administrative Privileges

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

- Installing or uninstalling the client on Windows 7 and higher with active UAC (User Access Control) requires the user to invoke the installer with the "run as administrator" option. To enable this right-click mouse option, add the following information to the registry:

```
[HKEY_CLASSES_ROOT\Msi.Package\shell\runas\command]
@=hex(2):22,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,05,02,00,6f,00,74,00,05,02,00,53,00,79,00,73,00,74,00,65,00,6d,00,03,03,00,32,00,5c,00,6d,00,73,00,69,00,65,00,78,00,65,00,6d,00,2e,00,65,00,78,00,65,00,22,00,20,00,2e,00,06,00,73,00,69,00,65,00,78,00,65,00,22,00,20,00,2e,00,06,00,05,02,00,0a,00,00,00
```

- To install or uninstall using the command line, the user must have administrator privileges ("run as administrator").

- Microsoft packages. During installation, the 1720 error message may occur:

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

Microsoft suggests this solution:

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

See also DES encryption on Windows 7 clients (on page 94)

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 24) 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
```
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.

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.
Working with Endpoint Security Policies

In This Section:

Overview of Endpoint Security Policy ................................................................. 65
Software Blades ..................................................................................................... 66
Protection for Servers ......................................................................................... 67
Working with Rules .............................................................................................. 68
Working with Policy Actions ............................................................................... 69
Policy Toolbar ........................................................................................................ 70
Enforcing Rules According to States ................................................................. 71
Installing Policy Changes on Clients ................................................................. 71
The Heartbeat Interval ......................................................................................... 72

Overview of Endpoint Security Policy

The Endpoint Security Policy is 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 Blades

The Endpoint Security policy can include rules for these Software Blades.

<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, Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• How a Full Disk Encryption user logs in to the computer</td>
<td>Windows, Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• How failed logins are handled</td>
<td>Windows, Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password security</td>
<td>Windows, Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access to remote help</td>
<td>Windows, Mac</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, Mac</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). Note - Port Protection is not supported on Mac OS.</td>
<td>Windows, Mac</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, Mac</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall</td>
<td>Blocks or allows network traffic based on attributes of network connections.</td>
<td>Windows, Mac</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, Mac</td>
</tr>
</tbody>
</table>
### Blade | Rule | Description | Client OS
--- | --- | --- | ---
Capsule Docs |  | Provides security classifications and lets organizations protect and share documents safely with various groups - internal and external. | Windows Mac
URL Filtering | URL Filtering | Lets organizations control access to websites by category, user or group. | Windows
SandBlast Agent Anti-Bot | SandBlast Agent Anti-Bot | Detects bot-infected machines and blocks bot C&C communication to prevent bot damage. Provides detailed information about the device affected by the bot activity, about the bot process itself, and other relevant information. | Windows
SandBlast Agent Forensics and Anti-Ransomware | SandBlast Agent Forensics and Anti-Ransomware | Analyzes incidents reported by other blades. Monitors files and the registry for suspicious processes and network activity. Prevents ransomware attacks. | Windows
SandBlast Agent Threat Extraction and Threat Emulation | SandBlast Agent Threat Extraction and Threat Emulation | Threat Emulation sends files on the endpoint computer to a sandbox for emulation to detect evasive zero-day attacks. Threat Extraction quickly delivers safe files while the original files are inspected for potential threats. | Windows
VPN | Remote Access VPN | Remote Access VPN lets users connect remotely to a Check Point Security Gateway using IPSec. | Windows Mac

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 all versions of Windows Server.

Do not deploy this Software Blade on clients that run operating systems that are not supported. You can also disable it in the policy.

To disable Software Blades on operating systems that are not supported:

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

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 (on page 44).

For supported servers see the Release Notes for your release.

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 34).
- Action definitions (on page 69) 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.
**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 Clear to show the full Rule Base.</td>
</tr>
</tbody>
</table>
## 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 > Endpoint Connection Settings**.
   
   The **Connection Settings 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. Click **Manage > Endpoint Connection Settings**.
   
   The **Connection Settings Properties** window opens.
2. In the **Out of Compliance** section, enter the number of heartbeats.
3. Click **OK**.
When you configure this time period, we recommend that you give users sufficient opportunity to:

- Save their data.
- Correct the compliance issues.
- Make sure that the endpoint computer is compliant.

The formula for converting the specified time period to minutes is:

\(<\text{number of heartbeats} > \times \text{heartbeat interval (in seconds)}\> \times 60.
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:

Use the instructions in the Installation and Upgrade Guide to install a Log Server.

Endpoint Policy Server Configuration

To define a new Endpoint Policy Server:

1. In SmartEndpoint, go to Manage > Endpoint Servers.
   The Endpoint Server window opens.
2. Click New.
   To edit an existing server, select it from the list and click Edit.
3. Enter Server Name and IP Address.
4. Select Endpoint Policy Server
5. Click Next.
6. Select an option to initiate secure trusted communication now or later:
   - **Initiate trusted communication** (If the servers are up and able to communicate)
     - Enter and confirm an Activation Key. You will enter this same key on the other servers.
     - Click Initialize.
   - **Skip and initiate trusted communication later** (If the servers are not ready to communicate)

7. Click Next.
   A warning pop-up window shows.

8. Click OK.

9. Click Finish.
   The Install Database window opens.

10. Wait for the database installation to finish.
    The Close button becomes available.

**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.
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 > Endpoint Connection Settings.
2. Enter or select the Interval between client heartbeats (on page 72) 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.
   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 (on page 72) 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 > Endpoint Connection Settings.
2. Clear Enable Endpoint Management Server to be Endpoint Policy Server.
3. Click OK.
4. Select File > Install Policies or click the Install Policies icon.

Policy Server and Management Server Communication

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

- Endpoint Policy Servers get from the Endpoint Security Management Server:
  - Policies and installation packages.
  - All files that it needs for synchronization.
- Endpoint Policy Servers send a heartbeat message to the Endpoint Security Management Server at 60 second intervals.
  You can change this in the $UEPMDIR/engine/conf/global.properties file on the Endpoint Security Management Server. The property name is connectionpoint.hb.interval.secs.
- Endpoint Policy Servers send sync messages to the Endpoint Security Management Server when synchronization is necessary.
- Endpoint Policy Servers send Reporting events to the Endpoint Security Management Server at 60 second intervals or when there are more than 1000 events in the queue.
  You can change this in the $UEPMDIR/engine/conf/global.properties file on the Endpoint Security Management Server. The property names are:
  - connectionpoint.emon.events.until.flush=1000
  - connectionpoint.emon.seconds.until.flush=60
- Endpoint Policy Servers send all database related messages directly to the Endpoint Security Management Server.

Notes on the First Synchronization

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

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

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

In This Section:
- Overview of Management High Availability ................................................................. 80
- Configuring a Secondary Server in SmartDashboard ................................................ 81
- Failover.......................................................................................................................... 82
- Synchronizing Active and Standby Servers ................................................................. 84
- Environments with Endpoint Security ......................................................................... 89
- Disaster Recovery with High Availability................................................................. 91

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.

This section contains general information about Check Point High Availability and information specific to Endpoint Security environments.

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 Server 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.

**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 (on page 82).
3. Change the Standby Security Management Server to Active (on page 82).

**If the Active Security Management Server has failed and you cannot change it:**

Manually change the Standby Security Management Server to Active (on page 82).

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

After you change the Standby Security Management Server to Active, edit the PAT version on the new Active Security Management Server (on page 90).

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Any</td>
<td>The SmartDashboard name of the server.</td>
</tr>
<tr>
<td>Type</td>
<td>Primary or Secondary</td>
<td>This is only the order of the installation and does not impact the environment.</td>
</tr>
<tr>
<td>Mode</td>
<td>Active or Standby</td>
<td>If the Security Management Server is currently <strong>Active</strong> or <strong>Standby</strong>.</td>
</tr>
<tr>
<td>Reachable</td>
<td>Yes or No</td>
<td>This field is only in the Peer Status. It shows if the local server has connectivity with that peer.</td>
</tr>
<tr>
<td>Status</td>
<td>Never been synchronized, Synchronized, Lagging, Database has been changed, Advanced, or Collision</td>
<td>The status of synchronization between the Security Management Servers. See Synchronization Status <a href="#">on page 88</a> for complete descriptions.</td>
</tr>
</tbody>
</table>

### Before Failover

Whenever possible, change the Active Endpoint Security Management Server to Standby before you change the Standby Endpoint Security Management Server to Active, and check online synchronization status on the Secondary server and all Remote Help servers.

**Notes** -

- A standby Endpoint Security Management Server cannot be changed to Active until the online synchronization is completed.
- While the Primary server is offline and the Secondary server is active, external Remote Help servers do not get updates.
To check online synchronization status:
Run this command on each server: `PgOnlineSyncUtil is_initial_load_over`
When the synchronization finishes, the command output is `Initial load is over`.

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**.

Also, see Manual Synchronization with Endpoint Security (on page 85).

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.

**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 89).

**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.

In 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

Online Automatic Sync

You can configure a new synchronization type, which synchronizes the Endpoint Security Management Servers each time the database is modified. This is called online synchronization.

To use online synchronization, all servers in the High Availability environment must be R77.20 or higher. Online synchronization is supported on Gaia servers only.

If there is one or more external Remote Help Server in an environment, you must use online synchronization.

To configure the secondary server with online synchronization:

1. In SmartDashboard, select Policy > Global Properties.
   The Global Properties window opens.
2. In the navigation tree, select Management High Availability.
3. Select **Manual synchronization only**.
4. Click **OK**.
5. In the **Network Objects** tree, right-click **Check Point** and select **Host**.
6. In the window that opens, enter a unique name and an IP address for the server.
7. In the **Software Blades** section, select the **Management** tab.
8. Select a policy management option:
   - **Network Policy Management** - the Secondary Server, Logging and Status, and Provisioning are selected automatically
   - **Endpoint Policy Management**
9. Click **Communication** to create SIC trust between the Secondary Endpoint Security Management Server and the Primary Endpoint Security Management Server.
10. In the window that opens enter these configuration parameters:
    - **One-time password** (twice to confirm) - SIC Activation Key that you entered in the Check Point Configuration Tool
    - Click **Initialize** to create a state of trust between the Endpoint Security Management Servers. If the trust creation fails, click **Test SIC Status** to see troubleshooting instructions
    - If you must reset the SIC, click **Reset**, then reset the SIC on the Secondary server and click **Initialize**
11. Click **Close**.
12. Click **OK**.
13. Select **File > Save**.
14. Select **Policy > Install Database**.
15. Select **Policy > Global Properties**.
    - The **Global Properties** window opens.
16. In the navigation tree, select **Management High Availability**.
17. Select **Automatic synchronization when policy is installed** and **Every time Endpoint Server database is modified**.
18. Click **OK**.
    - The synchronization begins.
19. Click **Save**.
20. To make sure the synchronization finishes, go to **Policy > Management High Availability**.
    - While synchronization continues, this warning shows: *Failed to receive current status. Reason: Synchronization is in progress. Try again Later*. When synchronization finishes, the status of the Secondary server changes to **synchronized**.
    - **Note** - If Remote Help servers are present, the status of the Secondary server remains **Never synchronized** until Database installation.
21. Select **Policy > Install Database**.
22. Do steps in Synchronizing MSI Files and Drivers (on page 89).

**Running Migrate in Online Synchronization Environment**

If a configuration was exported during Automatic Synchronization, you must re-configure it after the import.

Best practice is to re-install all Secondary Servers and Remote Help Servers after the migrate import procedure.
Install new Secondary Servers and Remote Help Servers of the same version as the primary server and synchronize all servers.

You must delete the previous Secondary and Remote Help Server objects in SmartDashboard Network Objects, and create new objects in SmartDashboard for the new servers.

Use the *R77 Installation an Upgrade Guide* and Environments with Endpoint Security (on page 89).

**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.

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

High Availability environments with Endpoint Security have some differences from other High Availability environments:

- The initial manual synchronization
- Failover
- Synchronization of MSI files and drivers
- Optional: Configure automatic sync on database change

⚠️ 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.

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 file 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:
      
      `$FWDIR/conf/SMC_Files/uepm/msi`

   b) On the Standby Security Management Server, replace theses folders with the folders that you copied from the Active Security Management Server:
      
      `$FWDIR/conf/SMC_Files/uepm/msi`

   c) If necessary, manually copy the Smart Card drivers:
      
      `$FWDIR/conf/SMC_Files/uepm/DRIVERS`

   d) Run:
      
      (i) `cd $FWDIR/conf/SMC_Files/uepm`

      (ii) `chmod -R u+rwx,g+rwx,o-rwx msi -`

      (iii) `find msi/ -type d -exec chmod g+s {} ;`
2. On the Standby Security Management Server, replace these folders with the folders that you copied from the Active Security Management Server:

$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:

   ```
   Gaia: uepm patver set <old_PAT_version_number> + 10
   ```
3. To make sure the new PAT version is set, run:

   ```
   Gaia: uepm patver get
   ```

### Deleting a Server

You can delete a Remote Help server or a Secondary Endpoint Security Management Server. Before you do that, make sure none of the remaining servers have connectivity to the deleted entities.

### 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. 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.

See: Recovery by Promoting a Secondary Server [on page 91].

Recovery by Promoting a Secondary Server

After your Primary server becomes permanently unavailable:

1. Promote the Secondary server to Primary.
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.

\\textbf{Note} - While the Primary server is off line and the Secondary server is active, Endpoint Security Remote Help servers do not get updates.

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.

Primary server acts as the synchronization master. It synchronizes the databases of one Secondary Endpoint Security Management Server and the master Remote Help server. All other Remote Help servers synchronize their databases with the Remote Help master. The synchronization speed depends on the network and the hardware characteristics.
Important - When Primary server is down, the Remote Help servers cannot synchronize their databases, until a Secondary server is promoted to Primary and the initial sync is finished. While the servers are re-syncing, the Remote Help server is unavailable. Therefore, we recommend that you schedule promoting a Secondary server to the Primary during non-working hours.

Before you promote a Secondary Endpoint Security Management Server to the Primary one, make sure they are synchronized.

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. Make a backup of the objects_5_0.C file.
3. Edit the objects_5_0.c file:
   a) Edit the Primary Object definitions to look like this:
      :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)
4. To change the registry and set this server to be the Primary server, run: cpprod_util FwSetPrimary 1
5. 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.
6. Make sure you have a mgmtha license on the newly promoted server.
   Note - All licenses must have the IP address of the promoted Security Management Server.
7. Run cpstart on the promoted server.
8. In SmartDashboard, select the Secondary server.
9. Select Change Active.
   If SmartDashboard fails to connect, reboot the server.
10. In SmartDashboard:
   a) Remove all instances of the old Primary Management object. To see all of the instances, right-click the object and select Where Used.
      Note - When you remove the old Primary server, all previous licenses are revoked.
   b) Install database.
Active Directory Authentication

In This Section:

- Endpoint Security Active Directory Authentication ..................................................... 93
- Configuring Authentication .......................................................................................... 94
- Configuring Active Directory for Authentication ......................................................... 94
- Configuring Global Authentication............................................................................... 95
- Strengthening the LDAP Communication ................................................................... 96
- Troubleshooting Authentication in Server Logs ........................................................... 98
- Troubleshooting Authentication in Client Logs............................................................ 99

Endpoint Security Active Directory Authentication

When an Endpoint Security client connects to the Endpoint Security Management Server, an authentication process identifies the endpoint client and the user currently working on that computer.

The 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` from `C:\Windows\System32`.

- 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` (in princ command: the first time in lower case and the second in upper case)
- `realm`: `NAC1.COM` (domain name)
- `userName`: `auth-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 (0x32ed87dbd5f0d5e9c8a8547376818d4)
```

**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.

**Notes** -
- Make sure that the time is less than 5 minutes apart on all Endpoint Security servers and the Kerberos server. If an Endpoint Security server and the Kerberos server are more than 5 minutes apart, a runtime exception shows and AD authentication fails.
- On Gaia - Use NTP or a similar service.
- To use Capsule Docs with Single Sign-on, disable User Access Control on Windows Active Directory Servers.

**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 > Endpoint 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 (on page 94).

<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. This value must match what was done in Active Directory &gt; <strong>New Object</strong>.</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 in the <strong>etype</strong> field.</td>
</tr>
<tr>
<td>Key version number</td>
<td>Enter the version number according to the Active Directory output in the <strong>vno</strong> field.</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 (on page 41).

### Strengthening the LDAP Communication

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

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

1. Open the `$UEPMDIR/engine/conf/ldap.utils.properties` file.
2. Configure the protocol or protocols to use.
   - **To configure LDAPS** - Change `use.ssl=false` to `use.ssl=true`
   - **To configure GSSAPI** - Change `use.gssapi=false` to `use.gssapi=true`

Both LDAPS and GSSAPI can be set to true.

3. Save.

For GSSAPI, no additional configuration is necessary.
Additional steps for LDAPS:

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

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

1. Find the index of the SSL certificate: On a domain controller which is configured to support LDAPS, run: `certutil -store -v MY`
   
   The output of this command is a list of certificates. The certificates are separated by a line like this:
   
   `================ Certificate 0 ================`, where 0 is the index number of the certificate.

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

3. Get that certificate’s index number this is number which appears in separation header before each certificate (in this example it is 0).

   `================ Certificate 0 ================`
   
   X509 Certificate:
   
   Version: 3
   Serial Number: 610206fb000000000002
   Signature Algorithm:
   
   Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
   Algorithm Parameters:
   
   05 00
   Issuer:
   
   CN=mulberry-DC-CA
   DC=mulberry
   DC=com
   NotBefore: 23/06/2014 13:12
   NotAfter: 23/06/2015 13:12
   Subject:
   
   **CN=DC.mulberry.com**
   Public Key Algorithm:
   
   ...
   Certificate Extensions: 9
   
   1.3.6.1.4.1.311.20.2: Flags = 0, Length = 22
   Certificate Template Name (Certificate Type)
   DomainController
   2.5.29.37: Flags = 0, Length = 16
   Enhanced Key Usage
   
   Client Authentication (1.3.6.1.5.5.7.3.2)
   
   **Server Authentication (1.3.6.1.5.5.7.3.1)**

4. Download a certificate from the domain controller:

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

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

5. Import a certificate to Endpoint Security servers. Copy the file to the Endpoint Security servers (primary and secondary) and run:

   `cd $UEPMDIR/engine/jre`
./bin/keytool -import -keystore ./lib/security/cacert -file <cert file name> -alias <alias>

For example: ./bin/keytool -import -keystore ./lib/security/cacert -file /certif/DCCert.cer -alias DCSSLCert


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 Gaia server:
2. Restart the Endpoint Security server.

Results in Authentication.log

- If the Authentication.log file on the server shows:
  ```
  ERROR: Config file contains no principals.
  ```
  The database was cleaned or the process to include authentication in the client package was faulty. To fix:
  a) Repeat the process to configure authentication (on page 94).
  b) Make a new client package.
  c) Restart the Endpoint Security server.

- If the Authentication.log file on the server shows:
  ```
  Permission denied in replay cache code
  ```
  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:

  ```plaintext
  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 (on page 94).

## 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:

```plaintext
[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.
Server and Client Communication

In This Section:

- Overview of Server and Client Communication ........................................................ 100
- SHA-256 Certificate Support ...................................................................................... 100
- TLSv1.2 Support .......................................................................................................... 101

Overview of Server and Client Communication

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

For example, the Endpoint Security Management Server enforces and updates policies on the Endpoint Security clients. Endpoint Security clients 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.

Endpoint Security Management Servers can communicate with Endpoint Policy Servers to distribute the load of client-server communication between multiple servers.

All Endpoint Security and other Check Point servers communicate with each other through internal SIC secure communication that uses certificate authentication. By default the certificates use SHA-1 encryption, but you can also configure SHA-256 encryption.

Endpoint Security Servers and clients communicate through TLSv1 and TLSv1.2 encryption.

SHA-256 Certificate Support

For clean installations, the management certificate can be encrypted with SHA-256 encryption. In existing R77.x environments and lower environments, SHA-256 is not supported for the Root CA. You can use SHA-256 for renewed certificates after the previous certificate expires. See sk103840 http://supportcontent.checkpoint.com/solutions?id=sk103840 for more information.

To activate a certificate with SHA-256 on a new installation:

1. Install a new Endpoint Security Management Server.
2. On the Endpoint Security Management Server, run: c pca_client set_sign_hash sha256
   
   This command changes the certificate hash to SHA-256 from SHA-1, which is the default.
3. Run: fwm sic_reset
   
   This command resets the internal CA.

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

4. Run: cpconfig and select Certificate Authority > Initialize.
   
   The new Internal CA certificate is created and signed with SHA-256.

5. Run: cpstart
6. Install this release.
7. Connect to the Endpoint Security Management Server with SmartDashboard and enable the **Endpoint Policy Management** blade.

**To configure a renewed certificate to use SHA-256:**

On the Endpoint Security Management Server, run: `cpca_client set_sign_hash sha256`  
After the management certificate expires, the renewed certificate will be signed with SHA-256 encryption.

### TLSv1.2 Support

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

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

1. On each Endpoint Security server, open `$UEPMDIR/apache22/conf/ssl.conf`.
2. Run: `cpstop`
3. Change the attribute `SSLProtocol +TLSv1 +TLSv1.2` to: `SSLProtocol TLSv1.2`
4. Save changes.
5. Run: `cpstart`
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 export with the path to the output (.tgz) file.
For example: `./migrate 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 import` with the full path to the input (.tgz) file.
   
   For example: `./migrate import <input_file_name>`

   The migrate utility:
   - Extracts the configuration files from the tgz.
   - Copies them to the correct places.
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:
   
   `Gaia - $UEPMDIR/bin`
3. Run the Endpoint Security Management Security utility (`uepm.exe`) and set the new PAT version:
   
   `Gaia: $UEPMDIR/bin>uepm patver set <old_PAT_version_number> + 10`
4. Make sure the new PAT version is set by running:
   
   `Gaia: $UEPMDIR/bin>uepm patver get`
Full Disk Encryption

In This Section:

- Overview of Full Disk Encryption ............................................................... 104
- Configuring Full Disk Encryption Policy Rules .............................................. 104
- Full Disk Encryption Installation and Deployment ........................................ 113
- Full Disk Encryption Recovery ..................................................................... 115
- Full Disk Encryption Self-Help Portal ........................................................... 118
- Full Disk Encryption Troubleshooting .......................................................... 120

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.

Configuring Full Disk Encryption Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

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

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>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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:
  - XTS-AES (256-bit) - Only available for UEFI-systems. Best practice is not to use this in environments with both UEFI and BIOS systems, as BIOS systems will default back to AES-CBC.
  - XTS-AES (128-bit) - Only available for UEFI-systems. Best practice is not to use this in environments with both UEFI and BIOS systems, as BIOS systems will default back to AES-CBC.
  - AES-CBC (256-bit) - Default
  - Blowfish (256-bit)
  - Cast (128-bit)
  - 3DES (168-bit)

- **What is encrypted:** By default all drives that are detected after the installation and all visible disk volumes are encrypted. IRRT devices are not encrypted.

To change the volumes and devices that are encrypted, select these options:

- To have only minimum encryption for Pre-boot protection, select **Minimum volumes for Pre-boot authentication**.
- To select the exact drives that are encrypted, select **Custom Volume Encryption** and click **Configure Volumes**.
- To encrypt volumes that are found after the initial Full Disk Encryption installation on a computer, select **Allow encryption of volumes that were detected after the initial installation**.
- To encrypt IRRT devices, select **Allow protection/encryption on IRRT devices**.
- To use a Self-Encrypting drive (SED), select **Allow using the hardware encryption functionality of self-encrypting drives**.
  Self-Encrypting drives encrypt and decrypt immediately.

**Custom Disk Encryption Settings**

If you select **Custom Volume Encryption** for the **Encrypted disks and volumes** setting, configure the encryption and Pre-boot settings for each volume.

To configure the settings for each volume:

1. In the **Custom Volume Encryption Settings** window, click **Add**.
2. Select the disk number and volume number to configure.
3. To enable Pre-boot on the volume, select **Pre-boot**.
4. To encrypt the volume, click **Encrypt**.
5. Click **OK**.
**Self- Encrypting Drives**

The disk encryption setting **Allow Self-Encrypting Drives (SED) hardware functionality** lets Full Disk Encryption probe and use SED disks that comply with the OPAL standard. If a compatible system and disk are detected, Full Disk Encryption uses the hardware encryption on the disk instead of the traditional software encryption.

When SED encryption is in effect on a client computer, the **Drive Information** in the **Encryption Status** of the client shows SED added to the volume name. You can see this in the Client UI and in the **Computer Details > Full Disk Encryption** in SmartEndpoint.

- AES encryption is always used with SED drives.
- You cannot use custom volume encryption with SED drives. The client overrides custom volume configuration.
- Manage SED drives in the same way as software-encrypted drives.

See the **Endpoint Security Release Notes** for this version for SED Requirements.

**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 107). 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.

Instead of no Pre-boot authentication, you can use:

- Single Sign-On (SSO) together with Pre-boot Authentication.
- Pre-boot with **Bypass Pre-boot when connected to LAN**.
- **Display Last Logged on User in Pre-boot** - The username of the last logged on user shows in the Pre-boot logon window. That user only needs to enter a password or Smart Card pin to log in.
- **Use TPM for Pre-boot integrity** - In E80.60 and higher clients this uses the TPM security chip to measure Pre-boot components. If they are not tampered with, the TPM allows the system to boot. See sk102009 [http://supportcontent.checkpoint.com/solutions?id=sk102009](http://supportcontent.checkpoint.com/solutions?id=sk102009) for more details.

  **Note**: The software based hardware hash is disabled when TPM is configured.

  You can also use TPM in addition to Pre-boot authentication for two-factor authentication. See Advanced Pre-boot Settings (on page 109).

If you do choose **Do not authenticate user before OS loads (disable Pre-boot)** without the precautions listed above, we recommend that you require Pre-boot authentication in some scenarios. See Temporarily Require Pre-boot (on page 108).

**Integrate with OS login** - If you do not require Pre-boot you can select this to have users log in to Windows only. It does not have the security of Pre-boot.

### Temporary Pre-boot Bypass

Temporary Pre-boot Bypass lets the administrator disable Pre-boot protection temporarily, for example, for maintenance. It was previously called Wake on LAN (WOL).

You enable and disable Temporary Pre-boot Bypass for a computer, group, or OU from the computer or group object. The Pre-boot settings in the Full Disk Encryption policy set how Temporary Pre-boot Bypass behaves when you enable it for a computer.

Temporary Pre-boot Bypass reduces security. Therefore use it only when necessary and for the amount of time that is necessary. The settings in the Full Disk Encryption policy set when the Temporary Pre-boot Bypass turns off automatically and Pre-boot protection is enabled again.

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

- Temporary Pre-boot Bypass
- Temporary Pre-boot Bypass from a script
- Temporary Pre-boot Bypass when connected to LAN

**To temporarily disable Pre-boot on a computer:**

1. In the Computer Details or Node Details window, select **Security Blades** > **Full Disk Encryption**. Or, right-click a node and select **Full Disk Encryption** > **Disable Pre-boot Protection**.
2. Click **Temporarily Disable Pre-boot**.
3. Click **Yes**.

The Pre-boot is enabled again when you click **Revert to Policy Configuration** or when the criteria in the Temporary Pre-boot Bypass settings are met.
To configure Temporary Pre-boot Bypass settings:

1. In a Full Disk Encryption rule in the Policy, right click the Authenticate before OS loads Pre-boot Action and select Edit Shared Action.
2. Click Temporary Pre-boot Bypass (Wake on LAN) settings.
3. Select the type of Temporary Pre-boot Bypass to allow:
   - Allow Temporary Pre-boot Bypass (Wake On LAN)
   - Allow bypass script. Also see Temporary Pre-boot Bypass with a Script (on page 108).
   - Allow bypass when connected to LAN
4. Click the link next to the option to configure when the selected type of Temporary Pre-boot Bypass occurs: By Demand, Once, or Weekly.
5. Select the date and time.
6. In Temporary Pre-boot Bypass duration, select when Temporary Pre-boot Bypass functionality become disabled. You must select one or both options.
   - Disable after X automatic logons - Select this to turn off the bypass after the configured number of logins to a computer.
   - Disable after X days or hours - Select this to turn off the bypass after the configured amount of time passed.

   After the number automatic logons occur or the number of days or hours expires, Temporary Pre-boot Bypass is disabled on the client and the Pre-boot environment shows. Select a small number so that you do not lower the security by disabling the Pre-boot for a long time.
7. Click OK.

   **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.

**Temporary Pre-boot Bypass with a Script**

If you run scripts to do unattended maintenance or installations (for example, SCCM) you might want the script to reboot the system and let the script continue after reboot. This requires the script to turn off Pre-boot when the computer is rebooted. Enable this feature in the Temporary Pre-boot Bypass Settings windows. The Temporary Pre-boot Bypass script can only run during the timeframe configured in Temporary Pre-boot Bypass Settings.

This is supported in E80.60 clients and higher on E80.60 and higher management.

**Running a Temporary Pre-boot Bypass script**

In a script you execute the FdeControl.exe utility to enable or disable Pre-boot at the next restart:

- Run: FDEControl.exe set-wol-on to enable Temporary Pre-boot Bypass.
- Run: FDEControl.exe set-wol-off to disable Temporary Pre-boot Bypass.

The above commands will fail with code 13 (UNAUTHORIZED) if executed outside the timeframe specified in the policy.

**Temporarily Require Pre-boot**

If you do not require Pre-boot, users go straight to the Windows login. Because this makes the computer less secure, we recommend that you require Pre-boot authentication in some scenarios.
To temporarily require Pre-boot:

1. In a Full Disk Encryption rule in the Policy, right click the Do not authenticate before OS loads Pre-boot Action and select Edit Properties.

2. Configure these options to Require Pre-boot authentication if one or more of these conditions are met:
   - **More than X failed logon attempts were made** - If a user’s failed logon attempts exceed the number of tries specified, Pre-boot is required. The computer automatically reboots and the user must authenticate in Pre-boot.
   - **The hard disk is not used by the original computer (hardware Hash)** - If selected, the client generates a hardware hash from identification data found in the BIOS and on the CPU. If the hard drive is stolen and put in a different computer, the hash will be incorrect and Pre-boot is required. The computer reboots automatically, and the user must authenticate in Pre-boot.
     
     **Warning**: Clear this option before you upgrade BIOS firmware or replace hardware. After the upgrade, the hardware hash is automatically updated to match the new configuration.
   - **The computer cannot reach any of the configured locations** - Requires Pre-boot when Location Awareness requirements are not filled. If you select this, configure the locations that the computer tries to reach in the list below.

3. **Before Pre-boot authentication is required, show this message** - Enter a message to display to the user if a configured condition is met and Pre-boot is required. For example, to call the Help Desk if the Pre-boot window opens.

4. Click **Use TPM for Pre-boot integrity** to use the TPM security chip available on many PCs during pre-boot in conjunction with password authentication or Dynamic Token authentication. The TPM measures Pre-boot components and combines this with the configured authentication method to decrypt the disks. If Pre-boot components are not tampered with, the TPM lets the system boot. See sk102009 http://supportcontent.checkpoint.com/solutions?id=sk102009 for more details.

**Advanced Pre-boot Settings**

You can set these Pre-boot Environment Permissions in the properties of the Pre-boot Protection action in a Full Disk Encryption policy rule. The hardware related setting are only for systems with BIOS firmware and do not affect systems with UEFI.

Note - These permissions are also in the Pre-boot Customization Menu on client computers. To open the Pre-boot Customization Menu:

- **On BIOS systems** - Press both shift keys on a client computer while Full Disk Encryption loads during the start up.
- **On UEFI systems** - Press the Ctrl and Space key on the computer keyboard.

<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>Permission</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Enable mouse in Pre-boot environment (BIOS only)</strong></td>
<td>Lets you use a mouse in the Pre-boot environment.</td>
</tr>
<tr>
<td><strong>Allow low graphics mode in Pre-boot environment (BIOS only)</strong></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 TPM two factor authentication (Password & Dynamic Tokens)** | Select to use the TPM security chip available on many PCs during pre-boot in conjunction with password authentication or Dynamic Token authentication. The TPM measures Pre-boot components and combines this with the configured authentication method to decrypt the disks. If Pre-boot components are not tampered with, the TPM lets the system boot. See sk102009 [http://supportcontent.checkpoint.com/solutions?id=sk102009](http://supportcontent.checkpoint.com/solutions?id=sk102009) for more details. |
| **Firmware update friendly TPM measurements** | Disables TPM measurements on Firmware/BIOS level components. This makes updates of these components easier but reduces the security gained by the TPM measurements because not all components used in the boot sequence are measured. If this setting is enabled on UEFI computers, the Secure Boot setting is included in the measurement instead of the firmware. |
| **Enable Remote Help** | Select to let users use Remote Help to get users access to their Full Disk Encryption protected computers if they are locked out. |
| **Remote Help response length** | Configure how many characters are in the Remote Help response that users must enter. |
User Authorization before Encryption

Full Disk Encryption policy settings enable user acquisition by default. If user acquisition is disabled, the administrator must assign at least one Pre-boot user account to each client computer before encryption can start.

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
- 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 lock screen authentication (OneCheck)**.
2. Optional: Configure the Check Point Endpoint Security screensaver.
   - The screensaver is active only after a Full Disk Encryption policy has been installed on the client.
   - After selecting the Check Point Endpoint Security screensaver option, enter the:
     - Text that shows when the screensaver is active.
     - Number of minutes the client remains idle before the screensaver activates.
3. Optional: Select **Require that only an authorized Pre-boot user is allowed to log into Windows**. If selected, only users that have permission to authenticate to the Pre-boot on that computer can log on to the operating system.
4. Optional: Select **Use Pre-boot account credentials in OS lock screen**. If selected, users authenticate in the regular Operating System login screen but with the credentials configured for Pre-boot.

Best practice is to only use this feature when there is no Active Directory available. For customers that use Active Directory, we recommend a combination of User Acquisition, OneCheck Logon, and Password Synchronization that will let users use the same credentials for Pre-boot and Windows login.
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

Note - Not all the Full Disk Encryption (FDE) requirements are shown here. For the complete FDE requirements, see the Release Notes for your Endpoint Security client version [http://supportcontent.checkpoint.com/solutions?id=sk117536].

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.
• Hybrid Drive or other similar Drive Cache Technologies. See sk107381 [http://supportcontent.checkpoint.com/solutions?id=sk107381].
• The root directory cannot be compressed. Subdirectories of the root directory can be compressed.

Other Requirements:

• All disks that are encrypted by FDE must have the same format (MBR or GPT)
• GPT-formatted disks are supported only on UEFI devices.

• If using “Fast start-up” on Windows 10 laptops, see sk140232.

• Update the BIOS on the client computer to the latest version.

• If using the the BIOS\UEFI option Fastboot, follow the precautions in sk140215

• If using a third-party credential provider to log in to Windows, configure FDE to use (wrap) the
  third-party provider. See sk118817

Upgrading Full Disk Encryption

If you upgrade Endpoint Security from an earlier version of R80, R80.x, or E80.x, no special actions
are required for Full Disk Encryption.

To upgrade Full Disk Encryption:

You must follow these procedures:

1. Upgrading Endpoint Security Clients [on page 58]
2. How to upgrade Windows 8 to Windows 8.1 with Full Disk Encryption in place (sk99064)
3. How to upgrade to Windows 10 1607 and above with FDE in-place (sk120667)

What effect does an upgrade have on users?

The upgrade does not have a significant effect on users.

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>
<tr>
<td>Filter driver</td>
<td>Prot_2k.sys</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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 115)** - 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.

- **Full Disk Encryption Drive Slaving Utility (on page 117)** - Use this to access specified files and folders on the failed, encrypted disk that is connected through a USB cable from a different “host” system.

- **Dynamic Mount Utility (on page 118)** - 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\n
2. 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.

Using Drive Slaving Utility

Full Disk Encryption Drive Slaving Utility lets you access Full Disk Encryption protected disk drives that become corrupted as a result of an Operating System failure. The Drive Slaving Utility is hardware independent, and can access hard disks connected through USB ports.

Full Disk Encryption Drive Slaving Utility replaces older versions of Full Disk Encryption drive slaving functionality, and supports R73 and all E80.x versions. You can use the Full Disk Encryption Drive Slaving Utility instead of disk recovery.

The utility is supported in E80.60 clients and higher on E80.60 and higher management.

Notes -

- On an E80.x client computer with 2 hard disk drives, the Full Disk Encryption database can be on a second drive. In this case, you must have a recovery file to unlock the drive without the database.

- Remote Help is available only for hard disk authentication. It is not available for recovery file authentication.
Before You Use the Drive Slaving Utility

Before you run the Full Disk Encryption Drive Slaving Utility, make sure to do these:

- Authenticate the Full Disk Encryption encrypted disk
- On systems with active Pre-boot Bypass, you must authenticate with Full Disk Encryption account credentials

We recommend that you use a recovery file when you are not sure if the hard disk drive or the Full Disk Encryption internal database on your system are corrupted.

Using the Drive Slaving Utility

To use the Full Disk Encryption Drive Slaving Utility:

1. On a computer with Check Point Full Disk Encryption installed, run this command to start the Full Disk Encryption Drive Slaving Utility: `<x:>`\Program files(x86)\CheckPoint\Endpoint Security\Full Disk Encryption\fde_drive_slaving.exe
   
   Note - To unlock a protected USB connected hard disk drive, you must first start the Drive Slaving Utility, and then connect the disk drive.

   The Full Disk Encryption - Drive Slaving window opens.

2. Select a Full Disk Encryption protected disk to unlock.
   
   Unlock volume(s) authentication window opens.

3. Enter User account name and Password.

4. Click OK.

After successful authentication, use Windows explorer to access the disk drive. If you fail to access the locked disk drive, use the Full Disk Encryption Recovery file, then run the Drive Slaving Utility again.

   Note - To prevent data corruption, shut down the system or use a safe removal utility before you disconnect the USB connected drive.

Dynamic Mount Utility


Full Disk Encryption Self-Help Portal

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

The portal is available for desktop and mobile devices.

Activating the Self-Help Portal

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

**Note** - On the [Gaia portal > Hosts and DNS](#) page, make sure to configure:

- The DNS Server
- Domain Name
- DNS suffix

To enable the Self-Help Portal:

On the Endpoint Security Management Server, run:

```bash
cd $UEPMDIR/engine/jre/bin/
selfhelp_cmd enable
```

Note that this restarts the Endpoint Security Management Server.

After activation, the Self-Help Portal is available at `http://<eps_server_ip>/eps_shp`

where `<eps_server_ip>` is the IP address of the Endpoint Security Management Server.

To disable the Self-Help Portal, run:

```
selfhelp_cmd disable
```

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

```
selfhelp_cmd status
```

Configuring the Self-Help Portal

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

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

To configure Self-Help Portal settings in SmartEndpoint:

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

Users can register to the Self-Help Portal and use it to recover passwords. The portal address is `http://<eps_server_ip>/eps_shp`

where `<eps_server_ip>` is the IP address of the Endpoint Security Management Server.
User Settings for the Self-Help Portal
You can force users to re-register to the Self-Help Portal or block users from recovering password in the portal.

To change a user’s settings for the Self-Help Portal:
1. In SmartEndpoint, in the Users and Computers tab, right-click on a user and select User Authentication (OneCheck).
2. Select Reset Self-Help Enrollment to force the user to re-register to the portal.
   Select Lock Password Self-Help to prevent users from recovering passwords in the portal.
3. A confirmation message shows. Click Yes.

Monitoring the Self-Help Portal Policy
To see the status of user enrollment and recovery for the Self-Help Portal:
In SmartEndpoint, in the Reporting tab, select User Authentication Policy > Self Help Status.

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:
   \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 7 and higher</td>
<td><code>C:\ProgramData\CheckPoint\Endpoint Security\Full Disk Encryption</code></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*. 
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.
   - 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.
OneCheck User Settings

In This Section:

Overview of OneCheck User Settings ................................................................. 125
Configuring OneCheck User Settings Policy Rules ............................................. 125
Before You Configure Smart Card Authentication ......................................... 134
Changing a User’s Password ............................................................................ 136
Managing Dynamic Tokens .............................................................................. 136

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.

Configuring OneCheck User Settings Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select New to define a custom Action option.

Right-click an Action and select Edit or Edit Shared Action to change the Action behavior.

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

Pre-boot Authentication Methods

If the Pre-boot is required on a computer as part of Full Disk Encryption, users must authenticate to their computers in the Pre-boot, before the computer boots. Users can authenticate to the Pre-boot with these methods:
• **Password** - Username and password. This is the default method.
  The password can be the same as the Windows password or created by the user or administrator.

• **Smart Card** - A physical card that you associate with a certificate. This is supported in E80.30 clients and higher.
  Users must have a physical card, an associated certificate, and Smart Card drivers installed.

• **Dynamic Token** - A physical device that generates a new password each time users start their computers. This is supported in E80.60 clients and higher on E80.60 and higher management.
  This can be configured for specified users and not as the global Pre-boot authentication method.

Configure the global settings for the Pre-boot authentication method from the OneCheck User Settings Actions.

### Global Pre-boot Authentication Settings

Configure the global settings for the Pre-boot authentication method from the OneCheck User Settings policy rule. The settings configured here apply to all users. You can override the global settings for specified users.

Select an Action to define the default Pre-boot authentication method:

<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 134). 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 [https://supportcenter.checkpoint.com](https://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.

On E80.60 and higher Endpoint Security Management Servers and E80.60 and higher clients, you can assign **Dynamic Token** as a user’s authentication method.

**To change a user Pre-boot authentication method:**

1. Double-click a user in the tree.
2. In the **User Details** window, select **OneCheck User Settings**.
3. Click **Pre-boot Authentication Method**.
4. Click **Use specific Pre-boot Authentication Method for this user**.
5. Select an authentication method:
   - **Password** - This user can only authenticate with a username and password.
   - **Smart Card** - This user can only authenticate with a Smart Card.
   - **Either Smart Card or Password** - This user can authenticate with user name and password or a Smart Card.
   - **Dynamic Token** - This user can only authenticate with the password from a dynamic token.

6. If you select **Smart Card**, we recommend that you select **Change authentication method only after user successfully authenticates with a Smart Card**.

   This lets users authenticate with a password until all of the requirements for Smart Card authentication are set up correctly. After users successfully authenticate one time with a Smart Card, they must use their Smart Card to authenticate. If you configure a user for Smart Card only and do not select this, that user is not able to authenticate to Full Disk Encryption with a password.
Select one or more Smart Card drivers.

7. If you select Dynamic Token, click **Select token**. The user can only authenticate with the selected token. See Managing Dynamic Tokens (on page 136).
   - Select a token from the list or click **Add** or **Import** to add a new token.
   - Click **OK**.

8. Click **OK**.

9. On the **OneCheck User Settings** page:
   - For **Password** authentication - You can enter a **User Password** or **Change Password**.
   - For **Smart Card** authentication - In the **User Certificates** area, make sure the user has a valid certificate to use with the Smart Card. If a certificate is not shown, you can click **Add** to import a certificate.

### Password Complexity and Security

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</td>
<td>The standard Windows password requirements are enforced:</td>
</tr>
<tr>
<td>complexity</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</td>
<td>If you select this, select the requirements for which type of</td>
</tr>
<tr>
<td>complexity</td>
<td>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: ! &quot; # $ % &amp; ' ( ) * + , - .</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>
</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: ! &quot; # $ % &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</td>
<td>Enter the minimum number of days that a password must be valid before the user can change it.</td>
</tr>
<tr>
<td>only after</td>
<td></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>
<tr>
<td>Number of passwords</td>
<td>Enter the minimum number of password changes needed before a previously used password can be used again.</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 OS Password Change</td>
<td>When the OS password on a computer changes, the Pre-boot password is automatically changed.</td>
</tr>
<tr>
<td>Update OS 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 OS 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 OS passwords</td>
<td>The Pre-boot and OS passwords on a computer are not synchronized by Endpoint Security.</td>
</tr>
</tbody>
</table>

In E80.60 and higher clients, Update OS Password Upon Pre-boot Password Change can include scenarios where the Pre-boot password is reset through Remote Help. To enable OS password change in this scenario, you must select Allow OS password reset on Pre-boot password reset in the Password Synchronization action window.

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:

<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>

**Logon Settings**

OneCheck User Settings **Logon Settings** define additional settings for how users can access computers. Expand the **Advanced section** in the OneCheck User Settings rule to configure this.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow logon to system hibernated by another user</td>
<td>Lets a different user than the logged on user authenticate in Pre-boot to a system in hibernate mode.</td>
</tr>
</tbody>
</table>
| **Allow use of recovery media** | Let user authenticate to use recovery media to recover and decrypt data from an encrypted system.  
*Note:* In E80.20 and higher, if this is not selected, users can still access recovery media that is created with a temporary user and password. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow user to change his credentials from the endpoint client</strong></td>
<td>Let users change the password on an endpoint client during the Pre-boot.</td>
</tr>
<tr>
<td><strong>Allow Single Sign-On use</strong></td>
<td>Let users use Single Sign On to log on to Pre-boot and Windows when OneCheck Logon is disabled. Single Sign on applies only to Pre-boot and Windows and not to different blades, such as VPN or Media Encryption. Users are always allowed to use Single Sign On when OneCheck Logon is running.</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>
Managing Authorized Pre-boot Users and Nodes

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

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

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

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

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

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

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

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

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

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

Creating Pre-boot Users

Pre-boot users can be within a node or not assigned to a node.

To create new online Pre-boot user:

1. in the **Users and Computers** tab, right-click on an OU under **Directories** or **Other Users/Computers**.
2. Select **User Authentication (OneCheck) > Authorize Pre-boot Users**.
3. Click **New**.
   - The **Add new Pre-boot user** window opens.
4. Enter a **Logon Name**
5. In the **Authentication credentials** area, select **Password** or **Dynamic Token**.
   - A password must contain at least five characters
   - If you select a token as the authentication method, make sure you select an existing token

6. To set more granular account controls, open **Account Details**.
   - **Do not use device information for Full Disk Encryption remote help** - Enables user-bound remote help for the pre-boot user
   - **Lock user for preboot** - Locks the user for preboot
   - **Require change password after first logon** - Applies only to password authentication.
     - Select this option to force users to change their password after the first Pre-boot logon.

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

   **To unlink a Windows user from the logged on Pre-boot account:**
   1. From an Endpoint Security client, open the client **Overview** and click on the **Full Disk Encryption Blade** icon.
   2. Click **Unlink**.
   3. Enter the password of the logged on Pre-boot account.
   4. Click **Unlink**.
      - A new link is created with a different Windows account at the next Windows log in.

**AD Groups for Pre-boot Authentication**

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

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

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

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

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

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

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

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

   If you try to add an entity that will bring the total number of users over 250, the operation is blocked.

### Before You Configure Smart Card Authentication

Make sure the environment is set up correctly to use Smart Card authentication before you configure it.

To use Smart Card authentication, you must have these components and requirements:

- **Smart Card authentication** is only supported on Endpoint Security clients of version E80.30 or higher. Make sure all users have a supported version.

  You can see which versions users have in the **Endpoint Security Management Console > Monitoring tab > Versions in Use**.

- Users must have the physical Smart Card in their possession.

- Users’ computers must have a Smart Card reader driver and token driver installed for their specific Smart Card. Install these drivers as part of the global **Pre-boot Authentication Settings**.

- Each user must have a certificate that is active for the Smart Card.

  - The Directory Scanner can scan user certificates from the Active Directory. Configure this in the global **Pre-boot Authentication Settings**.
  
  - You can manually import a certificate for a user in **User Details > Security Blades > OneCheck User Settings**.

- In a Full Disk Encryption Policy rule, open the **Authenticate user before OS loads** action. Click on **Advanced Pre-boot Settings** and make sure that **Enable USB devices in pre-boot environment** is selected.

### Smart Card Scenarios

Below are scenarios of how to implement Smart Card authentication in organizations with different needs.

#### Scenario 1: Moving from Password to Smart Card

**Scenario**

Your organization uses Check Point Endpoint Security with username and password authentication for Full Disk Encryption Pre-boot. You want to move all users to Smart Card authentication for even greater security. Your organization uses Active Directory.
What to do:

1. Plan your Smart Card environment:
   - Give all users a Smart Card.
   - Get a Smart Card certificate for each user and put them in Active Directory.
   - Learn which Smart Card driver and Reader driver is necessary for your Smart Card.

2. Upgrade all endpoints to this version. Use Reporting reports to make sure all users are successfully upgraded.

3. Open the Policy tab.

4. In a OneCheck User Settings rule, right-click the Authenticate users action and select Edit:
   - Select Smart Card (requires certificates).
   - Select Change authentication method only after user successfully authenticates with a Smart Card.
   - Select the drivers required for your Smart Card.

5. In the Directory Scanner area, click Configure.
   The Certificate Scanning Configuration window opens.

6. Select Scan user certificates from Active Directory.

7. Monitor the Smart Card deployment in the Pre-boot Reporting reports.

8. If you choose, you can clear the Change authentication method only after user successfully authenticates with a Smart Card option after all users have logged on with their Smart Card. If a specified user must use password authentication temporarily, you can change the Pre-boot Authentication Settings for the user to Password.

Scenario 2: Mix of Password and Smart Card Authentication

Scenario

Your organization is preparing to install Check Point Endpoint Security for the first time. Most users will use username and password Pre-boot authentication. Administrators with high administrative privileges will use Smart Card authentication. Your organization does not use Active Directory.

What to do:

1. Plan your Smart Card environment.
   - Give a physical Smart Card to all users who will use a Smart Card.
   - Get a Smart Card certificate for each user who will use a Smart Card.
   - Learn which Smart Card driver and Reader driver is necessary for your Smart Card.

2. Deploy the Endpoint Security client, including Full Disk Encryption on all endpoints, as described in the Deploying Endpoint Security Clients chapter (on page 47). Use Reporting reports to make sure that Full Disk Encryption completes the deployment phase and the Full Disk Encryption Status of each computer is Encrypted.

3. Open the Policy tab.

4. In a OneCheck User Settings rule, select one of the Authenticate users actions:
   a) Select Authenticate users with Password and manually configure the Smart Card users to use Smart Card authentication.
   b) Select Authenticate users using Smart Card or Password. For added security, you can manually configure each Smart Card user to use Smart Card authentication only.
5. Right-click the **Authenticate users** action and select **Edit**.

6. Select the drivers required for your Smart Card and the Smart Card protocol. All users will receive these settings, including those who are configured to use Password authentication.

7. In the OneCheck User Settings page for each Smart Card user, in the **User Certificates** area, click **Add** to import a certificate.

8. Monitor the Smart Card deployment in the Pre-boot Reporting reports.

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

**Notes on Using Smart Cards**

- Check Point does not supply Smart Card features to use with Windows. You can use third-party software, supplied by Windows or the Smart Card vendor.
- To use recovery media with a Smart Card-only user, when you create the recovery media, create a temporary user who can authenticate to it.

**Changing a User's Password**

Users can change their own passwords from the Pre-boot. You can manage user Pre-boot passwords from the **User Details** window.

To change a user’s Pre-boot password from SmartEndpoint:

1. In the **User Details > Security Blades > OneCheck User Settings** in the Pre-boot authentication method area, click **Change Password**.
2. In the **Change User Password** window, enter the new password and re-enter it.
3. Click **OK**.
4. Click **OK**.
5. Select **File > Save**.

**Managing Dynamic Tokens**

Manage the tokens that users can use in the SmartEndpoint.

**Adding a Token**

To add a dynamic token:

1. In SmartEndpoint, go to **Manage > Dynamic Token Management**.
2. Click **Add**.
   
   The **Add Token** window opens.
3. Enter relevant values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Valid parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Token Serial Number</td>
<td>Unique serial number identifying this token.</td>
<td></td>
</tr>
</tbody>
</table>
### OneCheck User Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Valid parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Algorithm</strong></td>
<td>Cryptography algorithm that this token implements.</td>
<td>DES 3DES</td>
</tr>
<tr>
<td><strong>Dynamic Token Key</strong></td>
<td>Token key used for this account.</td>
<td>DES: 14 characters long 3DES: 42 characters long Contains digits 0-9 and letters A-F</td>
</tr>
<tr>
<td><strong>Response Length</strong></td>
<td>Number of characters in the ASCII response string.</td>
<td>8 16</td>
</tr>
<tr>
<td><strong>Challenge Format</strong></td>
<td>Format of ASCII challenge string.</td>
<td>Hexadecimal Decimal</td>
</tr>
<tr>
<td><strong>Challenge Length</strong></td>
<td>Number of characters in the ASCII challenge string.</td>
<td>8 16</td>
</tr>
<tr>
<td><strong>Response Format</strong></td>
<td>Format of ASCII response string.</td>
<td>Friendly Decimal</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Optional text.</td>
<td>ASCII text</td>
</tr>
</tbody>
</table>

4. Click **OK**.

### Removing a Token.

To remove a dynamic token:

1. In SmartEndpoint, go to **Manage > Dynamic Token Management**.
2. Select a token you want to remove.
3. Click **Remove**.
   The token is removed immediately.
   
   **Note** - Once removed, a token cannot be restored.

### Importing Tokens

To import tokens:

1. In SmartEndpoint, go to **Manage > Dynamic Token Management**.
2. Click **Import**.
   The **Token Import Wizard** window opens.
   You can navigate to the location of the file through a windows explorer, by typing in a full path name, or drag and drop the file into the field in the wizard.
4. Click **Next**.
Tokens in the selected file show on the list.

5. Select tokens to import.
6. Enter the password for the .imp file.
7. Click Next.
   Decrypted tokens show on the list.
8. Select decrypted tokens.
9. Click Finish.

Upgrading Legacy Token Users

This upgrade helps resolve issues with users and systems in unmanaged legacy (pre-E80) token deployment environments.

To upgrade legacy token users to E80.60 or higher:

Media Encryption & Port Protection

In This Section:
- Media Encryption & Port Protection Terminology .................................................. 139
- Overview of Media Encryption & Port Protection ...................................................... 139
- Working with Actions in a Rule .................................................................................. 140
- Converting File Encryption Devices to Media Encryption ..................................... 160

Media Encryption & Port Protection Terminology

Storage Device - Removable media device on which users can save data files. Examples include: USB storage devices, SD cards, CD/DVD media and external disk drives.

Peripheral Device - Devices on which users cannot save data and that cannot be encrypted.

Device Category - Also called Device Class, an Industry standard device type that identifies the base functionality of a storage or peripheral device.

Media Owner - By default, this is the user who encrypts the device. If allowed by the policy, a different user can be assigned to be the media owner. This term applies only to users in Active Directory environments.

Business-Related Data - Confidential data file types that are usually encrypted in the business-related drive section of storage devices in Media Encryption & Port Protection.

UserCheck - Gives users a warning when there is a potential risk of data loss or security violation. This helps users to prevent security incidents and to learn about the organizational security policy.

Explorer Utility - Software that lets users read encrypted data on Endpoint Security-protected computers on which the Media Encryption 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 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** (on page 140) - Controls how users can read devices that are protected by the policy
- **Write Action** (on page 141) - Controls how and when users can write to devices that are protected by the policy
- **Peripheral Device Access** (on page 144) - Controls access to different types of peripheral devices

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

- **Offline Device Access** (on page 149) - Controls access to devices that are connected to a non-protected computer
- **Device Scanning and Authorization** (on page 152) - Configures scanning of storage devices for malware and unauthorized file types.
- **Log Actions** (on page 154) - Controls when Media Encryption & Port Protection creates log entries when a storage device is attached to an endpoint computer
- **UserCheck** (on page 155) - Controls when and how to tell users about policy violations and optionally lets them override a policy.
- **Site Actions** (on page 156) - Controls when to allow or prevent access to drives encrypted by different Endpoint Security Management Servers
- **Global Automatic Access** (on page 157) - 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><strong>Allow reading any data from storage devices</strong></td>
<td>Allow users to read encrypted and non-encrypted data from storage devices.</td>
</tr>
<tr>
<td><strong>Allow reading only encrypted data from devices</strong></td>
<td>Allow users to read only encrypted data from storage devices. Users cannot read unencrypted (Non-Business related) data.</td>
</tr>
<tr>
<td><strong>Do not allow reading from any storage device</strong></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 unencrypted data from storage devices - Users can read unencrypted (typically Non-Business Related) data.
   - Allow reading encrypted data from storage devices - Users can read encrypted (typically, but not always, Business Related data).
4. Add or change Settings for Specified Devices (on page 145).

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>Allow writing any data to storage devices</td>
<td>Users can write all file types to storage devices.</td>
</tr>
<tr>
<td>Encrypt business related data written to storage devices</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 142).</td>
</tr>
<tr>
<td>Encrypt all data written to storage devices</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>Do not allow writing any data to storage devices</td>
<td>Users cannot write any file types to storage devices.</td>
</tr>
<tr>
<td>Do not allow writing any data to storage devices, allow user override</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 do not select the **Log device events** option in the Media Encryption & Port Protection rule, log entries are not created even if the **Audit device events** option is selected in this window.

   - **Allow encryption** - Select this option to let users encrypt storage devices. If this option is cleared, no storage devices can be encrypted.

   - **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** [on page 143] 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** [on page 142] 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.
- **Text** - Plain text files

Groups defined as Non-Business Related by default

- **Multimedia** - Music and video files, such as MP3 or MOV
- **Image** - Vector image files such as JPG or PNG
- **Executable** - Executable program files, such as EXE or COM.

**To classify groups as Business or Non-Business Related:**

1. Click a write action and select **Edit Properties**.
2. In the **Removable Media Write Access** window, select **Encrypt business related data written to storage devices**.
3. Click the **Configure Business Related file types** link.
4. On the **Business Related File Types** page, select **Business-related** or **Non business-related**.
5. Click **Add** to add a group to the list.
6. Click **Remove** to remove a group from the list.

**Creating a Custom User Message**

You can customize the text that shows in all sections of the user message window, including the banner and the option buttons. You cannot change the Check Point logos. This feature is useful for translating user messages into different languages.
To create a custom user message:
1. In the Select User Message list, select New.
2. Enter a name and description in the applicable fields in the Policy Action Single Page Form window.
3. Optional: Select a language from the Language list. You can click Add to add another language to the list.
4. Select one or more text elements and enter your custom text.
5. Click Preview to see how the custom message shows on the screen.

Configuring Peripheral Device Access
Peripheral devices cannot be encrypted and do not contain storage. These predefined actions define which peripheral devices can be used with an endpoint computer.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow connecting essential devices</strong></td>
<td>Access to necessary peripheral devices for basic computer functionality is allowed. Other peripheral devices are blocked.</td>
</tr>
<tr>
<td>(keyboard, mouse, and network adapters)</td>
<td></td>
</tr>
<tr>
<td><strong>Block all transmitting devices</strong></td>
<td>Access to transmitting peripheral devices is blocked. Other peripheral devices are allowed.</td>
</tr>
<tr>
<td>(Modem, Bluetooth, IrDA, Wi-Fi)</td>
<td></td>
</tr>
<tr>
<td><strong>Allow connecting all peripheral devices</strong></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 (on page 144) and change (on page 145) 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 [on page 148] 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**.
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 141).
   - For Storage Device Read Access see Configuring the Read Action (on page 140).
   - 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 (on page 145).
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 141).
    • For Storage Device Read Access see Configuring the Read Action (on page 140).
    • 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 141).
   • For Storage Device Read Access see Configuring the Read Action (on page 140).
   • 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 (on page 145) 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???
4. 123456?
5. 1234567
Advanced Actions

In This Section

- Offline Access Actions ................................................................. 149
- Device Scanning and Authorization Actions .................................. 152
- Log Actions ...................................................................................... 154
- UserCheck Actions ......................................................................... 155
- Media Encryption Site Actions .......................................................... 156
- Global Automatic Access Action ......................................................... 157
- Upgrading Media Encryption R73.x Devices and Keys ......................... 158

Offline Access Actions

You can select one of these predefined actions to define encryption behavior for storage devices:

- **Allow offline access to encrypted media** - Users can enter a password to access storage devices on protected computers not connected to an Endpoint Security Management Server (Offline). Users can also use their password to access storage devices on a non-protected computer.

- **Do not allow offline access to encrypted media** - Users cannot access storage devices on protected computers that are not connected to an Endpoint Security Management Server or on non-protected computers.

You can change the settings of these predefined actions and create new custom **Offline Access to Media** action.

Custom Offline Access Settings

You can define custom offline access actions that include these settings:

Encryption Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to choose owner during encryption</td>
<td>Lets users manually define the device owner before encryption. This lets users create storage devices for other users. By default, the device owner is the user who is logged into the endpoint computer. The device owner must be an Active Directory user.</td>
</tr>
<tr>
<td>Allow user to change size of encrypted media</td>
<td>Lets users change the percentage of a storage device that is encrypted, not to be lower than Minimum percentage of media capacity used for encrypted storage or Default percentage of media capacity used for encrypted storage. Also see Configuring Encryption Container Settings (on page 151).</td>
</tr>
<tr>
<td>Allow users to remove encryption from media</td>
<td>Lets users decrypt storage devices.</td>
</tr>
<tr>
<td>Allow user to upgrade from legacy drives</td>
<td>Lets users upgrade storage devices that were encrypted by File Encryption version R73.</td>
</tr>
</tbody>
</table>
### Setting

<table>
<thead>
<tr>
<th>When encrypting, Non-Business Related Data will be:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When encrypting, Non-Business Related Data will be:</strong></td>
<td><strong>Select one of these actions for existing data on a storage device upon encryption:</strong></td>
</tr>
<tr>
<td><strong>Copied to encrypted section</strong> - Non-Business Related data is encrypted and moved to the Business Related (encrypted) storage device.</td>
<td>We recommend that you back up Non-Business Related data before encryption to prevent data loss if the encryption fails. For example, this can occur if there is insufficient space on the device.</td>
</tr>
<tr>
<td><strong>Deleted</strong> - Non-Business related data is deleted.</td>
<td></td>
</tr>
<tr>
<td><strong>Untouched</strong> - Non-Business Related data is not encrypted or moved.</td>
<td></td>
</tr>
</tbody>
</table>

| Secure format media before encryption | Run a secure format before encrypting the storage device. Select the number of format passes to do before the encryption starts. |

| Change device name and icon after encryption | When selected, after the device is encrypted, the name of the non-encrypted drive changes to **Non Business Data** and the icon changes to an open lock. When cleared, the name of the non-encrypted drive and the icon do not change after the device is encrypted. |

### Offline Access Settings

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

Configure options for setting the encrypted space on storage devices.

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

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

**To force encryption of all media:**

1. Do not select **Allow user to change the size of encrypted media**.
2. Set the **Minimum percentage** and **Default percentage** of **media capacity** to **100**.

**Password Constraints for Offline Access**

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

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

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

Double-click an action to edit the properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Use custom requirements** | If you select this, select the requirements for which type of characters the password must contain or not contain:  
   - Consecutive identical characters, for example, aa or 33  
   - Require special characters. These can be: ! ^ # $ % & ' ( ) * + , . / : < > ? @ {  
   - Require digits, for example 8 or 4.  
   - Require lower case characters, for example g or t.  
   - Require upper case characters, for example F or G.  
   - Password must not contain user name or full name. |
<p>| <strong>Minimum length of password</strong> | Enter the minimum number of characters for a valid password. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Number of passwords</td>
<td>Enter the minimum number of password changes needed before a previously used password can be used again.</td>
</tr>
</tbody>
</table>

**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><strong>Do not lock out storage device upon failed authentication.</strong></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><strong>Temporarily lock storage device upon failed authentication attempts</strong></td>
<td>After a configured amount of failed log on attempts (the default is 5), the device is temporarily locked.</td>
</tr>
<tr>
<td><strong>Permanently lock storage device upon failed authentication attempts</strong></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.

On E80.64 and higher clients, CDs and DVDs (optical media) can also be scanned.

**Note** - After a media device is authorized:

- If you make changes to the contents of the device in a trusted environment with Media Encryption & Port Protection, the device is not scanned again each time it is inserted.
- If you make changes to the contents of the device in an environment without Media Encryption & Port Protection installed, the device is scanned each time it is inserted into a computer with Media Encryption & Port Protection.
You can select one of these predefined options for a Media Encryption & Port Protection rule:

<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. In a Media Encryption & Port Protection rule, click a device scanning and authorization action and select Edit Properties.
2. Click the Configure unauthorized file types link.
3. In the Unauthorized File Types window, select a Mode:
   - Unauthorized - Configure the file types that are blocked. All other file types are allowed.
   - Authorized - Configure the file types that are allowed. All other file types are blocked.
   The default is unauthorized with all file types allowed.
4. Click Add to add file types to the list.
5. Select file types from the Available Objects list and click Add to move them to the Selected Objects list.
   - If you selected Unauthorized mode, select the file types that are not blocked from storage devices.
   - If you selected Authorized mode, select the file types that are allowed on storage devices.
6. Optional:
   - Click New to create a new file type.
   - Click Remove to remove a group from the list.
7. Click OK.
8. Click OK.

To enable or disable scans for optical media (CDs and DVDs):

1. In a Media Encryption & Port Protection rule, click a device scanning and authorization action and select Edit Properties.
2. In the Device Overrides area:
   - To disable scans, select Exclude optical media from scan.
   - To enable scans, clear Exclude optical media from scan.
3. Click OK.
**Custom Scan and Authorization Actions**

You can create custom actions that have different requirements for authorization and the media scan. You can let users connect storage devices without a scan or delete unauthorized file types from the storage device.

**To define custom actions:**

1. Double-click an action in a rule and select the **New** action.
2. In the **Edit Properties** window, configure these parameters as necessary:

<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>
<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 (on page 145).
Log entries are initially stored on client computers and then uploaded to the server at predefined intervals.

**UserCheck Actions**

UserCheck for Media Encryption & Port Protection tells users about policy violations and shows them how to prevent unintentional data leakage. When a user tries to do an action that is not allowed by the policy, a message shows that explains the policy.

You can optionally let users write to a storage device even though the policy does not allow them to do so. In this case, users are prompted to give justification for the policy exception. This justification is sent to the security administrator, who can monitor the activity.

You can use the default UserCheck messages or define your own custom messages.

**To change an existing UserCheck message:**

1. Right-click a UserCheck action, and select **Edit**.
2. For each UserCheck message type, select an option to show a message. Clear an option to prevent a message from showing.
3. **Optional:** Click **Configure** to define a custom UserCheck message.
4. **Optional:** Click **Configure** to define a custom **Ask User** message.

**To define a custom UserCheck message:**

1. Right-click a UserCheck action, and select **Custom**.
2. Enter a unique name for the new action.
   You can optionally add text comments and select a display color.
3. Do steps 2 through 5 in the above procedure as necessary.
Media Encryption Site Actions

Site Actions control when to allow or prevent access to encrypted devices that were encrypted by different Endpoint Security Management Servers. Each Endpoint Security Management Server (known as a Site) has a Universally Unique Identifier (UUID). When you encrypt a storage device on an Endpoint Security client, the Endpoint Security Management Server UUID is written to the device. The Site action can prevent access to devices encrypted on a different Endpoint Security Management Server or from another organization. The Site action is enabled by default.

When a user attaches a storage device, Media Encryption & Port Protection makes sure that the device matches UUID the Endpoint Security Management Server UUID or another trusted Endpoint Security Management Server. If the UUIDs match, the user can enter a password to access the device. If the UUID does not match, access to the device is blocked.

This table shows what occurs when you insert an encrypted device into a client that is connected to an Endpoint Security Management Server the policy allows read-access. The Endpoint Security Management Server that the device was encrypted with is referred to as "the encrypting Endpoint Security Management Server".

<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 Endpoint Security Management Server. If you add Endpoint Security Management Servers to the table below, they are considered trusted and devices encrypted on those servers are allowed also.</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>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>All users in the organization can read encrypted data, only owners can modify</strong></td>
<td>All users can read encrypted files on storage devices. Only the media owner has can change encrypted content.</td>
</tr>
<tr>
<td><strong>Only owners can access encrypted data</strong></td>
<td>Only media owners read and/or change encrypted content.</td>
</tr>
<tr>
<td><strong>Access to encrypted data requires password authentication</strong></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
   - **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 E80.65 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.

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
"TcpPort"="1433"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp]
"TcpHideFlag"=dword:00000000
"TcpDynamicPorts"=""
"TcpPort"="1433"
"Enabled"=dword:00000001

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:

```sql
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**.
The Capsule Docs Software Blade, managed by an on-premises Security Management Server, lets organizations protect and share documents safely within the organization and with business partners, and manage the organizational Capsule Docs policy, monitoring, and deployment through SmartEndpoint.

Overview of Capsule Docs

Check Point Capsule Docs provides these benefits:

Control the parties that can access the data
- Restrict access to individuals, groups or entire organizations.
- Use granular Classification model to assign different permissions for internal and external users.
- Control data distribution (Forward, Copy/Paste, Print).
- Choose contacts from your Outlook address book with whom you usually communicate.
- Prevent unintentional data loss with the help of UserCheck.
- Use Data Classification to classify documents without encryption.
- Set a document expiration date to limit when documents can be accessed.

Protect data stored on untrusted servers and shared via untrusted channels
- Each protected document remains protected even on untrusted servers.
- Prevent forwarding to unauthorized parties.
- Secure all created documents automatically.
- Set a document expiration date.

See full audit trail for data access
- All actions on protected documents are logged and are available through SmartView Tracker and SmartLog.
- Follow paper trail for a single document.
- Audit distribution patterns for documents in an organization.
- Monitor access by external parties.
Access protected documents easily from your platform of choice
- Seamless integration with Microsoft Office and Adobe Acrobat on Windows platforms.
- Lightweight Windows Viewer that does not require administrative privileges or Microsoft Office or Adobe Acrobat clients installed.
- Access protected documents from proprietary Apps on Android, and iOS mobile devices.

Full Integration with Organizational Active Directory
- Users that are defined in the Active Directory are automatically provisioned to use Capsule Docs.
- User’s Active Directory account authentication is sufficient to access relevant protected documents.
- Customize Capsule Docs policy for different Users, Organizational Units and Groups.

You must configure all prerequisites before you can work with Capsule Docs.

Prerequisites for Capsule Docs

This picture gives an overview of the different components required for a Capsule Docs deployment as part of an Endpoint Security environment:

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Internal Network</td>
</tr>
<tr>
<td>1</td>
<td>Management Server</td>
</tr>
<tr>
<td>2</td>
<td>Active Directory Server</td>
</tr>
<tr>
<td>3</td>
<td>SMTP Server</td>
</tr>
<tr>
<td>4</td>
<td>Internal users</td>
</tr>
<tr>
<td>5</td>
<td>Management Console</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>DMZ</td>
</tr>
<tr>
<td>6</td>
<td>Reverse Proxy</td>
</tr>
<tr>
<td>7</td>
<td>Public-facing DNS Server</td>
</tr>
<tr>
<td>8</td>
<td>Mobile users</td>
</tr>
<tr>
<td>9</td>
<td>External users</td>
</tr>
</tbody>
</table>
Notes:

- **Management Server (1)** - A Secondary Management Server and Endpoint Policy Servers can be used for redundancy and load balancing.

- **Active Directory Server (2)** - Each user account in the Active Directory must have a valid email address. This is usually populated automatically if Microsoft Exchange is configured. User authentication fails if there are two AD accounts with the same email address.

- **SMTP Server (3)** - Is only required if the organization shares data with external users

- **SMTP Server (3)** with encryption protocols SSL and TLS are supported.

- **Reverse Proxy (6)**, and a **Public-facing DNS Server (7)** are only required if one or more of these conditions exist:
  - The organization shares data with external users.
  - Protected documents are accessed from mobile devices that do not have access to internal resources.

  If these conditions do not exist, a DNS Server is still required but does not need to be accessible from external networks.

To share protected documents externally, you must have an SMTP server and configure a Reverse Proxy.

Workflow for Capsule Docs Configuration

Before you configure Capsule Docs policy in SmartEndpoint:

2. Configure the Active Directory server as the primary DNS server (on page 164).
4. Prepare the Reverse Proxy (on page 165).
5. Configure an email server (on page 167).

Configuring the Primary DNS server

To configure the Active Directory server as the primary DNS server in Gaia:

1. In the Portal, **Network Management** navigation tree menu, select **Hosts and DNS**.
2. Enter the IP address of the Active Directory server as the **Primary DNS Server**.
3. Click **Apply**.

To configure the Active Directory server as the primary DNS server in Windows:

1. In the **Control Panel** window, go to **Network and Internet > Network and Sharing Center > Change adapter settings**.
2. Right-click the server network interface and select **Properties**. The **Connection Properties** window opens.
4. In the window that opens, enter the IP address of the Active Directory server as the **Preferred DNS server**.
5. Click **OK**.
6. Click **Close**.
Configuring the Directory Scanner

See Active Directory Scanner (on page 39) for instructions to configure the Directory Scanner.

Preparing the Reverse Proxy

The Reverse Proxy makes sure that requests from mobile devices and Capsule Docs clients that do not have internal network access reach the Endpoint Security Server.

If you use a Security Gateway as the Capsule Docs Reverse Proxy, do the procedures in this section. Alternatively, you can configure a third party server, for example an Apache Server, as a Reverse Proxy Server. See sk102973 http://supportcontent.checkpoint.com/solutions?id=sk102973 to use a third party server as a Reverse Proxy Server.

To prepare the Security Gateway for the Capsule Docs Reverse Proxy you must:

- Enable the Mobile Access Software Blade on the Security Gateway.
- Configure the Reverse Proxy on the Security Gateway or server to point to the Endpoint Security Management Server.
   
   **Note** - Make sure the name of the Endpoint Security Management Server resolves correctly in DNS.

- For Gaia: If the Gaia portal of the Mobile Access Security Gateway is on https://<gateway ip> with a “/” at the end and on port 443, you must change the URL or port. For example, change the URL to https://<gateway ip>/gaia or change the port to 4434. Change the URL in the Gateway Properties tree select Platform Portal and change the Main URL. This change requires a policy installation.
   If you do not make this change, the Gaia portal will not be accessible.

To enable the Mobile Access Software Blade on the Security Gateway:

1. In SmartDashboard that manages the gateway, double click the Security Gateway object.
2. In the properties window that opens, select Mobile Access in the Software Blades section.
   The Mobile Access Configuration wizard opens.
3. Click Cancel, if you want to use the Security Gateway as a reverse proxy only.
   The Mobile Access Policy is created, but has no rules in it.
4. Click OK.
5. In the main menu, go to Policy > Install.
6. Select the Security Gateway to install policy only on the Security Gateway.
   During policy installation, a warning shows: The Mobile Access Policy does not contain any rules. You can ignore this.
7. Click OK.
To configure the Capsule Docs proxy on the Security Gateway:

1. On the gateway, run:
   
   ```
   ReverseProxyCLI add application capsule_docs <public_server_name> <capsule_docs_server>
   ```

   Where:
   - `<public_server_name>` is the Capsule Docs Server public name, configured in SmartEndpoint. This hostname should be resolved to the Reverse Proxy Gateway, for example: capsuledocs.externalsite.com
   - `<capsule_docs_server>` is the Capsule Docs Server internal hostname OR IP address, for example: capsuledocs.internalsite.com OR 1.1.1.1

2. Follow the on-screen instructions.
   Make sure that the output of **Please wait.. Calculating your internal Host (host) IP addresses** is the IP address of the internal server and that no warnings are shown.

3. Run: `ReverseProxyCLI apply config`
   Make sure the command output is: **Finished applying configuration successfully.**
   If warnings are shown you must resolve the problems before you continue.

You can also enable Single Sign-on for Capsule Workspace with Capsule Docs users.

To enable Single Sign-on for Capsule Workspace Capsule Docs users:

1. In SmartDashboard, click the Mobile Access tab.

2. In the navigation tree, select Applications > Web Applications.
   The list of all Web Applications shows.

3. Click New.
   The Web Application window opens.

4. In the General Properties screen, enter the Name of the new Capsule Docs Web Application

5. In the Authorized Locations screen, select the Endpoint Security Management Server Host or the DNS name of the Endpoint Security Management Server.
   If it does not show in the drop-down menu, click Manage > New, select Host or DNS Name, and configure the new Endpoint Security Management Server.

6. In Directories section of the Authorized Locations screen, select Allow access to specific directories, and add new directories:
   a) Click New.
   b) In the window that opens, type in the directory path.
   c) Click OK.
   The new directories are:
   - /eps/client/services/DirectoryService
   - /eps/client/services/EpsCommonService
   - /eps/mobile/getDocumentKey
   - /eps/mobile/login
   - /policy

8. In the Link in Portal screen, configure these settings:
   a) Select Add a link to this Web application in the Mobile Access portal.
   b) In the Link text field, enter a label for the link. This does not affect users.
   c) Enter the URL https://<Endpoint Security Management Server IP or DNS IP address>
   d) In the Tooltip field, enter the external name of the Endpoint Security Management Server exactly as it is configured on the Endpoint Security Management Server.
9. In the Additional Settings > Single Sign-on screen, configure these settings:
   a) Select Turn on Single Sign-on for this application.
   b) Select Advanced for When a user signs in to this application.
   c) Click Edit.
   d) In the window that opens, select This application reuses the portal credentials. If authentication fails, Mobile Access prompts users and stores their credentials.
   e) Click OK.
   f) Click Edit in the Login Settings section.
   g) In the window that opens, select The users of this application belong to the following Windows domain, and enter the users’ domain name.
   h) Click OK.
10. In the Additional Settings > Link Translation screen, select Using the following method and Path Translation.
    Note - on gateway objects, Path Translation is supported by default.
11. Click OK.
12. Install Policy.

    Note - To grant access to an application for the Capsule Workspace users, you must add a Single Sign-on access rule to the Capsule Workspace policy.

Configuring a Mail Server for Capsule Docs

To send protected documents to external users, you must configure your email server. Two types of email servers are supported:

- SMTP (default)
- FileSystem

To configure the email server:

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

8. Click **OK** to save the email server settings and close the window.

**Troubleshooting issues with email settings**

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

1. In SmartEndpoint, select **Manage > Email Server Settings > Configure Settings**.
2. In the **Email Server Settings** window select **User authentication is required**.
   Configure these parameters:
   - **Port** - Leave the default (25).
   - **User Name** - Enter a fictitious email address. This address will show as the sender of email alerts.
   - **Password** - Enter a fictitious password. This is not used.
3. Optional: Trigger an alert to test the email server.

**Single Sign-on with Active Directory**

For managed clients to seamlessly authenticate to Capsule Docs with users’ AD credentials, enable Single Sign-on with Active Directory authentication. The default setting is **Do not allow Single Sign-on with Active Directory**.

To enable Single Sign-on with Active Directory:

1. Prepare the Active Directory server for authentication. Use the instructions in Configuring Active Directory for Authentication (on page 94).
2. Configure the authentication settings in SmartEndpoint. Use the instructions in Configuring Global Authentication (on page 95). To enable Capsule Docs Single Sign-on, it is not necessary to select **Work in authenticated mode**. We recommended that you do not select this option during the evaluation and lab stage.
3. Save.
4. In SmartEndpoint, **Policy** tab, in the **Capsule Docs** policy rules, select **Allow Single Sign-on with Active Directory**.
5. Install policy in SmartEndpoint.

**Using Capsule Docs**

When users create a new document in a supported application, the protection settings of their default Capsule Docs community are applied to the document. Users can change the settings through the Capsule Docs menu.

In some MS Office versions, the menu shows in the upper-right corner of documents. In others it shows in the Home tab.
Based on the Capsule Docs policy that you configure, users can:

- Change document Classification
- Change Community
- Remove protection
- Add or remove users and groups
- Set a document expiration date (only document Authors can do this)
- Create Favorites lists of users and groups.

**Note** - the Favorites lists can be used across the supported applications, to share the documents with different sets of users.


### Configuring Capsule Docs Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

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

Actions with the 🛠 icon apply to all of the organization.

### Organization Settings

The Organization Settings define the name of the organization and the name of the Public or External Server. This is the domain name that leads to the reverse proxy server or gateway.

**Note** - The Public Server Name should be configured one time and not changed.

### Active Classifications

Define the Capsule Docs classifications in use and the permissions associated with them.

Also define the permissions of document **Authors**. By default the permissions are set to be based on the classifications assigned to individual documents or higher. However, you can change them as necessary. A document can have multiple authors. **Classification based** means that the setting for the Author is the same as what is defined for the Classification.

**To create a new classification:**

- Click **Create Classification**.

**To delete a classification:**

- Click **Revoke Classification**.
To change the order of the classifications that end-users see in the Capsule Docs menu:

- Select a classification from the table and click the up and down arrows

For each Classification, define its properties and permissions in the table. For more details about the options see sk105076 http://supportcontent.checkpoint.com/solutions?id=sk105076.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Select the icon that users see in protected documents.</td>
</tr>
<tr>
<td>Classification Name</td>
<td>Give the classification a descriptive name.</td>
</tr>
</tbody>
</table>
| Applied On     | • **All Users** - The same definitions of the classification apply to All Users.  
                    • **Separate Internal and External Users** - There are different permissions for each classification, one for **Internal** and one for **External** users. When you select this, a second row opens for the classification. |
| Encrypted      | • **Yes** - Documents with this classification are encrypted and marked with a pink lock.  
                    • **No** - Documents are classified but not encrypted. There is no user list and all users can access the document. All permissions except **Unprotect** and **Change Classification** are changed to **Yes** automatically. |
| Edit           | Can users edit the document: **Yes** or **No**.                                                                                             |
| Modify Users   | Can users add or remove users and groups: **Yes** or **No**.                                                                                  |
| Change Classification | Can users change the classification of a document: **Yes** or **No**.                                                     |
| Unprotect      | Can users make a document unprotected: **Ask**, **Yes**, or **No**. If **Ask** is selected, users must give a reason if they choose to unprotect a document. |
| Mobile Access  | Can the document be accessed through Capsule Docs on mobile devices: **Yes** or **No**.                                                       |
| Print          | Can users print the document: **Yes** or **No**.                                                                                             |
| Screen Capture | Can users take screenshots of the document: **Ask**, **Yes**, or **No**. If **Ask** is selected, users must give a reason that they require screenshots. |
| Copy Paste     | Can users copy from the document and paste in their device: **Yes** or **No**.                                                            |
| Markings       | Double-click to change the selection. Select a header, footer, or watermark with the **Classification Name** to include in the document. Different markings are supported for different document types. |
Email Domains for Sharing Documents

Email Domains for sharing documents defines permissions for new user registration, based on email domains. Each domain can be defined as either Internal or External. There are two default domains that cannot be edited or deleted:

- **AD Scanned Domains** - Defined as Internal and contains users added by the Active Directory scanner.
- **Non AD Scanned Domains** - Defined as External and contains users that are not configured in the Domain Configuration window.

You can add more Internal or External Non AD Scanned Domains, and set the permissions to add New Users from them:

- Can register after explicitly added to a document
- Can register without being explicitly added to a document
- Not allowed

Automatic Protection

Define the default encryption behavior for new documents:

- Enforce automatic protection for new documents
- Do not enforce automatic protection
- Suggest document protection when saving document

You can also manually select or clear these options in the Properties of the Action:

- Protect new documents created by internal users
- Suggest to protect when user saves document
- Suggest to protect when user performs Save As

Initial Protection Configuration

Define the default protection settings that are assigned to newly protected documents. Users with the required permissions can edit these settings from the document.

The settings are:

- Select the classification, for example, Restricted or Highly Restricted.
  The classifications and permissions shown are those configured in the Classifications and Permissions Action. You cannot edit them from this Action.
- Add and remove user groups that show in newly protected documents.
- Configure which users or groups have Author permissions. The Document Protector is the person who first protects the document. This person can have Author permissions but it is not required. One or more entities must have Author permissions.
To add and remove user groups that show in newly protected documents:

1. Click the arrow and select **Manage Groups** to open the organizational tree and select one or more groups to add to the list.
2. Select one or more groups from the list. These groups are added to the initial protection list that is automatically assigned to a document.
   All groups that show in the Protection Setting window are assigned to the document.
3. To remove a group or user, select it from the list and click the **X**.

To configure which users or groups have **Author** permissions:

- Right-click the **Document Protector** or a different user or group and select an option:
  - **Remove as Document Author**
  - **Mark as Document Author**

If the default classification does not have encryption:
All users can access it and the users and groups selected here only apply if the classification is changed to one with encryption.

**Inviting Users**

Set permissions for the ability to add new users to a document if they are not yet invited or registered. By default, all users in the internal domains have permission to the documents and do not require invitations.

The options are:

- **Allow inviting users from any domain**
- **Do not allow inviting users**

If you select **Allow inviting users from any domain**, you can also limit the users who can be invited to those from specified domains.

To limit the users who can be invited to a document:

1. In a Capsule Docs rule, right-click the **Inviting Users** Action and select **Edit Shared Action**.
2. In the bottom part of the **Properties** window, in the **Permission to invite new users** list, select **Allow only from the following domains**.
3. Click **Add** to add domains to the list. Only users in domains on the list can be invited.

**Client Access Settings**

Configure Client access to protected documents.

Set the period of downtime, after which if the client does not get updated, the access to protected documents becomes blocked. You can also configure how often the client checks for updates.

**Single Sign-on with Active Directory**

This Action defines permissions for Single Sign-on with Active Directory. The default is **Do not allow Single Sign-on with Active Directory**.
Working with External Users

You can add external users who can access Capsule Docs protected documents in these ways:

- A user adds an external user to a document.
- An external user downloads the Capsule Docs client and registers.
- An administrator adds a user or domain in SmartEndpoint. The administrator can add individual users or import users from a .csv file.
  - Right-click the **External Users** folder in the Users and Computers tree and select **Capsule Docs > Add External Users**.
  - In the **Global Actions** pane, select **Add External Users**.

The first time that an external user from a new domain is added to the system, a new folder is created for the domain in the Users and Computers tree under **External Users**.

External users are in one of these states, shown in the **User Details**:

- **Invited** - A user added the external user to a document but the new user did not register yet.
- **Registered** - The user downloaded the Capsule Docs client and registered with an email address.
- **Revoked** - The administrator revoked the user and the user cannot log in to Capsule Docs or see documents. Revoked users are in the **Revoked Users** folder. Administrators can **Restore** or **Delete** users from there.

An administrator can give an external user or domain internal permissions.

**To give an external user the same permissions as an internal user:**

Right-click on a user or domain from the **Users and Computers** tree and select **Grant internal permission (for document use)**.

External users who have internal permissions are shown in the Capsule Docs internal users Virtual Group.

**To revoke an external user:**

Right-click on a user or domain from the **Users and Computers** tree and select **Revoke user**. The user is moved to the **Revoked Users** folder. You cannot delete external users.

Troubleshooting Capsule Docs Reverse Proxy

**Traffic Logs**

You can configure the Reverse Proxy to send traffic logs, which then can be reviewed in SmartLog, under Mobile Access logs.

**To configure the Reverse Proxy to send traffic logs:**

1. In SmartDashboard **Mobile Access** tab, go to **Additional Settings > Logging**.
2. In the **Tracking** section of the configuration screen, select **Log Access for Web Applications**, and select events to log:
   - **Unsuccessful access events**
   - **All access events**
3. Install Policy.

**Identify Reverse Proxy logs by these criteria:**

- **Category:** Mobile Access
- **Application:** Reverse Proxy

The **Access** section of the log can show:

- **Allowed - Authorized URL** - The Reverse Proxy allowed the URL request (only shows if the **All access events** logging option is configured)
- **Denied - Unauthorized URL** - The Reverse Proxy blocked the URL request. If this is a mistake, you can allow the URL.
  
  To allow a blocked URL:
  
  - In the command line, run: `ReverseProxyCLI show applications`
  - Under `capsule_docs app` in the **Paths** column, find the path that is unauthorized in the log.

- **Failed** - The Reverse Proxy failed to forward the request for the EPS with one of these messages:
  
  - **Internal Server Error** - The Endpoint Security Management Server aborted the connection with the gateway. Make sure the Endpoint Security Management Server is working.
  - **Proxy not found** - The given proxy host could not be resolved.
  - **Can't resolve host name** - The `<capsule_docs_server>` is the internal_host you configured in your `capsule_docs` application, you can see it under `ReverseProxyCLI show applications` in the **Internal Server Name** column.

  Your Endpoint Security Management Server is configured as a DNS name. Make sure that this hostname can be resolved from the gateway. To do this run `nslookup` on the host to see that the gateway can resolve it.

  - **Internal host connection failed** - Failed to connect to the internal server, make sure the server is up and running.
  - **Invalid URL** - The URL from the gateway to the Endpoint Security Management Server was not properly formatted.
  - **SSL handshake failed** - A problem occurred somewhere in the SSL/TLS handshake between the gateway and the Endpoint Security Management Server.
  - **Server response was too slow** - Operation timeout
  - **Page not found

- Action that the Reverse Proxy took in relationship to this URL - **Allowed, Denied, or Failed**

---

**Capsule Docs Recovery**

**Capsule Docs Recovery**

The Capsule Docs Recovery Tool generates a master key that can open all documents in a situation of disaster recovery.

A new master key is valid for one year. Therefore we recommend that you generate a new master key every year. A notification shows in the SmartEndpoint **Overview** page when the master key is close to its expiration date. A new master key can open all documents that were created before its creation and up to one year afterwards.
To get the Capsule Docs Recovery Tool:
1. In the SmartEndpoint, select Tools > Capsule Docs Recovery Tool.
2. In the window that opens, create a Recovery Key Password and enter it twice.
3. Click Save As and select a location where the Tool is saved in a zip file.
4. If necessary, extract the tool and use the included instructions.

Capsule Docs and Network DLP Integration
Capsule Docs and the Network DLP Software Blade integrate to provide these capabilities:

- **Content-aware file protection for network locations** - Protects files located on any CIFS and NFS-compatible network locations. It can apply protection settings based on the file contents. The engine scans a network location, defined in the policy, and applies relevant protection settings to files that match the filtering criteria. There is also file protection for Windows-based servers and workstations available with a standalone utility. For more information see the Capsule Docs Bulk Protection Reference Guide.

- **Content-aware protection for email attachments** - Protects email attachments in email messages that go through the gateway. It can apply protection settings based on the file contents, according to the policy.

Prerequisites for Capsule Docs with DLP
Before you configure content-aware file protection on network locations, make sure that:

- The Capsule Docs environment with a Capsule Docs policy is set up.
- To use content-aware protection for email attachments, make sure that a mail server is defined in the DLP settings. For details, see the *R77 Versions Data Loss Prevention Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=24852.
- There is at least 80KB of free space on the file server for each file you want to protect.

Deploy Capsule Docs with DLP on one Security Management Server for both Endpoint Security management and management of the Gateways.

Enabling Capsule Docs with DLP
To export the Endpoint Security Management Server certificate to the DLP Gateway for server authentication:

1. On the Endpoint Security Management Server, copy the file $UEPMDIR/engine/conf/ssl/root_sic_cert.pem
2. Put the file on the DLP Gateway in $FWDIR/cpcd/cert/
   
   **Note** - To disable server authentication (not recommended for a production environment), edit the file $FWDIR/conf/fwdsd.conf and change the value of cda_enable_server_authentication to false.
To enable Capsule Docs on a DLP Gateway:
1. In SmartDashboard, open DLP Gateway Properties window.
2. In the Software Blades section, select Capsule Docs under DLP.
3. In the navigation tree, go to Data Loss Prevention > Capsule Docs.
4. From the Endpoint Security Management list, select an Endpoint Security Management Server that is used to manage the Capsule Docs policy.
5. Enter the email address and password of a user in the Capsule Docs system. This user is used to log in to the Capsule Docs Server.
6. Click OK.
7. Install Policy.

Connecting the Security Management Server with Active Directory

To use Active Directory users and groups in the File Protection policy, create a new LDAP Account Unit that is connected to the Active Directory and make sure that this is the Active Directory that the Endpoint Security Management Server scanned.

To create a new LDAP Account Unit:
1. In SmartDashboard, double-click the management object to open its Object Properties window
2. In the Software Blades section, select Logging & Status and Identity Awareness.
3. Continue as prompted by the configuration wizard.
   For more information, see the Security Management Administration Guide.
4. Install Policy.

Configuring File Repositories

Configure the file repositories that Capsule Docs protects.

To configure a new file repository for Capsule Docs protection:
1. In SmartDashboard, open the Data Loss Prevention tab.
2. From the navigation tree, select Repositories.
3. Click New and select Fingerprint and File Protection.
   The Data Type Wizard window opens.
4. Type a name of the new file repository.
5. Click Next.
6. Enter settings for the files to scan:
   - Network path
   - Username
   - Password
7. Select Apply Capsule Docs Protection.
8. From the Install On drop-down menu, select a gateway that has Capsule Docs Software Blade activated.
9. From the File protection drop-down menu, select a file protection profile, or click New to create a new file protection profile.
   If you click New, the File Protection window opens. Configure the new protection profile.
settings:

- **Name** - Protection profile name.
- **Classification** - Capsule Docs classification to apply to protected documents.

The Capsule Docs classifications are defined in SmartEndpoint. To see the permissions associated with the selected classification, click View Permissions.

- **Protection Groups\Users** - Authorized users and groups. Click Add AD Entity and select an Active Directory user or group, or click Add Non-AD Entity > Non-AD User and enter an email address for a user or select a name of a Virtual Group defined in SmartEndpoint.

10. Click **OK**.
11. Click **Next**.
12. If you want to configure more data type properties, select **Configure additional Data Type properties after clicking Finish**.

The Data Type configuration window will open after the Data Type Wizard finished and the repository is created. For more information on available Data Type Wizard settings, see Data Loss Prevention Administration Guide.

13. Click **Finish**.

The new repository shows in the Repositories list.


## Starting a File Repository Scan

After you install the policy, you can run a manual scan or schedule future scans.

We recommend that you run the scan when network traffic is low, or run it on a dedicated gateway. You can also lower the priority of the scan process so that it does not affect other processes. See Troubleshooting Capsule Docs and DLP Integration (on page 178).

To start a scan manually:

1. In SmartDashboard, open the Data Loss Prevention tab.
2. From the navigation tree, select Repositories.
3. Select a repository from the list, and click Start Scan in the right pane.

The scan runs and the progress shows.

To configure a scan schedule:

1. In SmartDashboard, open the Data Loss Prevention tab.
2. From the navigation tree, select Repositories.
3. Select a repository from the list, and click Edit.
4. In the Data Type window that opens, select Scan Scheduling from the navigation tree and configure the schedule settings.
5. Click **OK**.

## Configuring Protection for Email Attachments

To configure Capsule Docs protection for email attachments:

1. In SmartDashboard, open the Data Loss Prevention tab.
2. From the navigation tree, select Policy.
3. Add a new rule:
   - In the Protocol column select Email.
   - Optional: In the Action column, we recommend that you select Inform User and create a new Inform User message that explains that the email attachment is protected with Capsule Docs.
   - In the Action column, right-click and select File Protection.
4. From the File protection list, select a file protection profile, or click New to create a new file protection profile.  
5. If you click New, the File Protection window opens. Configure the new protection profile settings:
   - Name - Protection profile name.
   - Classification - Capsule Docs classification to apply to protected documents. The Capsule Docs classifications are defined in SmartEndpoint. To see the permissions associated with the selected classification, click View Permissions.
   - Protection Groups\Users - Authorized users and groups. Click Add AD Entity and select an Active Directory user or group. You can also click Add Non-AD Entity > Non-AD User and enter an email address for a user or select the name of a Virtual Group defined in SmartEndpoint.
6. To dynamically add the mail sender and mail recipients in the document, click Non-AD Entity > Mail entity. If you use the same file protection object for repositories, the mail entities are ignored.
7. Click OK.
8. Install Policy.

Managing File Protection objects

To create, edit or delete File Protection objects:
1. In SmartDashboard go to Data Loss Prevention.
2. From the navigation tree, go to Additional Settings > File Protection.
3. Do one or more of these actions:
   - Create a new File Protections object
   - Edit an existing File Protections object
   - Delete a File Protections object
4. Install Policy.

Troubleshooting Capsule Docs and DLP Integration

Issue: Scan of network location consumes too much gateway resources.
When the DLP gateway runs a scan on the network location, it consumes a lot of gateway resources and can impact other processes on the gateway.
Solution: You can lower the priority of the scan process so that it does not affect other processes. This makes the scan and protection of files take longer to complete.
To lower the priority of the scan process:

1. On the DLP gateway open the `discovery.conf` file found under
   `$FWDIR/dlp/discovery/<UID of the repository>/discovery.conf`.
2. Change the value of `process_nice_value` from `-1` to `10`.

Issue: The repository scan summary log in SmartLog shows there are fewer protected files than the number scanned.

**Solution**: You can get the list of files that are not protected from the gateway to understand what was not scanned and why.

To get the names of failed files by connecting to the gateway:

1. Connecting to the gateway.
2. Open `$FWDIR/dlp/log/dlp_discovery_details.log`.
3. Search for these phrases:
   - **PROTECTION: SKIPPED** - Shows on files that are already protected or the file format is not supported.
   - **PROTECTION: FAILURE** - Shows for other types of errors.
Anti-Malware

In This Section:

- Prerequisites .............................................................................................................. 180
- Configuring Anti-Malware Policy Rules .................................................................... 181
- Submitting Malware and False Detections ............................................................... 186

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 and Cloud Reputation services.
- 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>
      ```

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.

Configuring Anti-Malware Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select New to define a custom Action option.

Right-click an Action and select Edit or Edit Shared Action to change the Action behavior.

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

Note that exclusions that you configure in one action apply to all Anti-Malware scans.

Scan All Files on Access

By default, all file are scanned when they are opened or used.

You can configure Trusted Processes as exceptions. When a trusted process accesses a file, the file is not scanned. Exclude a process only if you fully trust it and are sure it is not malware.

You can also select or clear these options:

- **Detect Unusual Activity** - Use behavior detection methods to protect computers from new threats whose information has not been added to the databases yet. It does not monitor trusted processes.

- **Enable Cloud Reputation Services For Files, Web Resources, and Processes** - Use cloud technologies to improve precision of scanning and monitoring functions. If you enable or disable this setting, it takes affect after the client computer restarts.

- **Connection Timeout** - Change the maximum time to get a response from Reputation Services (in milliseconds).

  **Note** - If you decrease this value, it can improve the performance of the Anti-Malware blade but reduces security, as clients might not get a reputation status that shows an item to be zero-day malware.

- **Enable Web Protection** - Prevents access to suspicious sites and execution of malicious scripts. Scans files, and packed executables transferred over HTTP, and alerts users if malicious content is found.

- **Mail Protection** - Enable or disable scans of email messages when they are passed as files across the file system.
To configure trusted processes:

1. In the **Properties** of the **Scan all files on Access** Action, click **Add**.

2. In the **Trusted Processes** window, enter the fully qualified path or an environment variable for the trusted executable file. For example:
   - `C:\Program Files\MyTrustedDirectory\MyTrustedProgram.exe`
   - `%programdata%\MyTrustedProgram.exe`

3. Click **OK**.
   The trusted program shows in the **Trusted Processes** list.

**Malware Signature Updates**

Anti-Malware gets malware signature updates at regular intervals to make sure that it can scan for the newest threats.

These Actions define the frequency of the signature updates and the source.

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

- **Signature update will fail after** - The connection timeout, after which the update source is considered unavailable.

- **Update Signatures From** - The server or servers that the client gets updates from.
  - **Signature Source:**
    - **Local Endpoint Servers** - Get updates from the Endpoint Security Management Server or configured Endpoint Policy Server.
    - **External Check Point Signatures Server** - Get updates from an external Check Point server through the internet.
    - **Other External source** - Get updates from an external source through the internet. Enter the URL.

- **If first update fails** - Set a fallback update source to use if the selected update source fails. Select a different option than the first signature source.

- **If second update fails** - Set a second fallback update source to use if the other sources fail.

**Note** - If only **Update from Local Endpoint Servers** is selected, clients that are disconnected from an Endpoint Security server cannot get updates.
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\n   - 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.

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.
Overview of Forensics and Anti-Ransomware

The SandBlast Agent Forensics and Anti-Ransomware Software Blade monitors file operations, processes, and network activity for suspicious behavior. It also analyzes attacks detected by other client blades or the Check Point gateway. It applies remediation to malicious files.

Anti-Ransomware constantly monitors files and processes for unusual activity. Before a Ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

All details of attacks are organized in the Forensics Analysis Report.

For example, if SandBlast Agent Anti-Bot detects a malicious URL, it notifies Forensics through internal communication. Forensics starts a complete investigation and generates a Forensics Analysis Report.

You can also configure the Forensics blade to analyze incidents that are detected by a third party Anti-Malware solution.

Configure the settings in the SandBlast Agent Forensics and Anti-Ransomware rule of in the SmartEndpoint Policy tab.

If Endpoint Security servers do not have internet connectivity, Forensics information is stored and sent for evaluation immediately when a server connects to the internet.

Anti-Ransomware Files

SandBlast Agent creates honeypot files on client computers to better detect ransomware before it starts to encrypt the user’s files.
These are the files that SandBlast Agent creates:

- MyMusic\00Fin\**AR*.bmp
- MyMusic\00Fin\BB*.gif
- MyMusic\**AAAA*.jpg
- MyMusic\Check*In.png
- MyDocuments\00Fin\MyDoc*.doc
- MyDocuments\00Fin\MyDoc*.docx
- MyDocuments\wahoo*o.rtf
- MyDocuments\**.txt
- PublicVideos\00Fin\MyMovie*.wmv
- PublicVideos\00Fin\MyMovie*.mp3
- PublicVideos\wahoo*o.wmv
- PublicVideos\**.mp3
- PublicPictures\00Fin\**AR*.bmp
- PublicPictures\00Fin\BB*.gif
- PublicPictures\00Fin.jpg
- PublicPictures\Check*In.png
- PublicDocuments\00Fin\MyDoc*.doc
- PublicDocuments\00Fin\MyDoc*.docx
- PublicDocuments\wahoo*o.rtf
- PublicDocuments\**.txt

If a file is deleted, it is automatically recreated after the next system boot.

**Configuring Forensics and Anti-Ransomware Policy Rules**

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

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

The **Default Forensics settings** rule applies to the **Entire Organization**. You can edit the default rule, but you cannot delete it.

**Automatic Threat Analysis Settings**

Define the automatic threat analysis settings in the **Triggers and Automatic Response** Action.

The automatic options are:

- **Automatically analyze threats** - Analyze incidents based on Check Point’s recommended triggers (default).
- **Automatically analyze and remediate infections** - Analyze incidents based on Check Point’s recommended triggers and apply remediation automatically.
- **Do not analyze threats** - Automatic Forensics analysis is turned off.

You can edit the selections manually to define when these processes occur.

The confidence level is how sure Endpoint Security is that a file is malicious. High confidence means that it is almost certain that a file is malicious. Medium confidence means that it is very likely that a file is malicious.

- **Forensics Analysis** - When Forensics analysis occurs.
- **File Quarantine** - When files are quarantined for Threat Emulation and Anti-Bot.
- **Machine Quarantine** - When machines are quarantined. If a computer is quarantined, the Firewall restricts network access.
- **Attack Remediation** - When remediation occurs for components that are part of an attack.
To granularly edit which type of events trigger a Forensics response:

1. In a SandBlast Agent Forensics and Remediation rule, right-click the **Automatic Threat Analysis** Action and select **Edit Shared Action**.
2. Click **Override confidence level per specific event**.

You can override the settings of the rule for up to five different events.

The Triggers include:

- Events detected by Endpoint Security Software Blades: Anti-Bot, Threat Emulation, Anti-Malware
- Events detected by Network Software Blades: Anti-Bot, Threat Emulation, Anti-Malware, URL Filtering

### Configuring Network Blades for Forensics Triggers and Remediation

To make triggers and remediation work for events detected by Network Threat Prevention Software Blades, you must configure gateway policy for the Threat Prevention blades: Anti-Bot, Anti-Virus, and Threat Emulation.

Each blade must be enabled and have Protection settings of **Prevent** or **Ask**, which include UserCheck.

Best practice is to use the **Threat Prevention Recommended Profile** (default) that includes all required settings.

### Monitoring and Exclusions

Define which processes are monitored by the Forensics blade.

In the default monitoring settings, processes with certificates from some trusted companies are excluded.

You can **Add**, **Edit**, and **Remove** exclusions from the list.

**To exclude a process from monitoring:**

1. From a SandBlast Agent Forensics and Anti-Ransomware rule in the **Policy**, right-click the **Monitoring and Exclusions** action and select **Edit Shared Action**.
2. Click **Add exclusion**.
3. In the window that opens select:
   - **Process** - To exclude an executable. You can also include Certificate information.
     - In **Process name**, enter the name of the executable.
     - Optional: Enter more information in the fields shown **Signer** is the company that signs the certificate. The more information you enter, the more specified the exclusion will be.
   - **Certificate** - To exclude processes based on the company that signs the certificate, for example, Google.
     - In **Certificate Data**, enter a name of company that signs certificates, or browse to add a certificate file.
4. Click **OK**.
5. The exclusion is added to the Exclusions list.
Disk Space for Forensics

By default, Forensics uses up to 1 GB of disk space on the client computer for data. You can configure more space for Forensics storage, but not less.

After the threshold is reached, the oldest data is deleted.

Change the **Maximum Forensics Database** size in the **Disk Usage** area of the **Monitoring and Exclusions** Action.

You can configure more settings related to space usage in GuiDBedit Tool (see sk13009 [http://supportcontent.checkpoint.com/solutions?id=sk13009](http://supportcontent.checkpoint.com/solutions?id=sk13009)) or dbedit (see sk13301 [http://supportcontent.checkpoint.com/solutions?id=sk13301](http://supportcontent.checkpoint.com/solutions?id=sk13301)).

**Important** - Do NOT use these tools unless instructed by Check Point Support or R&D. Incorrect use may corrupt settings in the management database.

Quarantine Settings and Attack Remediation

Define what happens to the components of an attack that is detected by Forensics. When files are quarantined, they are deleted and put in a secure location from which they can be restored, if necessary.

The automatic options are:

- **Quarantine all attack elements** - All components of the attack are quarantined.
- **Quarantine only files with known malicious reputation** - If a file is not known as malicious, it is not quarantined.

You can manually edit the treatment for each category of file: **Malicious**, **suspicious**, or **unknown**. For each category, you can select:

- **Quarantine** - Files are deleted and put in a secure location from which they can be restored, if necessary.
- **Delete** - Files are permanently deleted.
- **Backup** - Delete the file and create an accessible duplicate.
- **None** - No action is taken.

**Trusted Files** are those defined as trusted by the Check Point Reputation Service. The remediation options for **Trusted Files** are:

- **Terminate** - Stop the suspicious process.
- **Ignore** - Do not terminate processes. Activity is monitored.

File Quarantine Settings

Define the settings for files that are quarantined.

In the Default File Quarantine Settings, files are kept in quarantine for 90 days and users can permanently delete items from quarantine.

You can edit the Quarantine settings:

- **Click Add exclusion** to exclude a file or process from quarantine. You can define an exclusion by many different criteria. Criteria include: File extension, certificate data, MD5 hash, and SHA1 hash. Add more information to make the exclusion very specific and less information to make it broad.
• **Keep file in quarantine for** - Select the number of days that files are kept in quarantine before they are permanently deleted.

• **Quarantine folder name** - Select the quarantine location on client computers.

• **Copy quarantine files to a central location** - Enter a central location that quarantined files from client computers are copied to.

• **Allow users to delete items from quarantine** - When selected, users can permanently delete items from the quarantine file on their computers.

• **Allow users to restore items from quarantine** - When selected, users can restore items from the quarantine file on their computers.

### Anti-Ransomware Backup Settings

When Anti-Ransomware is enabled, it constantly monitors files and processes for unusual activity. Before a Ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

Define settings for Anti-Ransomware backup and restoration.

**General Anti-Ransomware Settings**

• **Enable Anti-Ransomware** - This is selected by default. To disable Anti-Ransomware, clear it.

• **Automatic restore and remediate** - When selected, Anti-Ransomware automatically starts remediation after a Ransomware attack. It deletes files created by the attack and restores the original files.

When this is not selected, users must start the restoration from the client computer. See Manual Anti-Ransomware Restoration (on page 192).

• **Restore to selected location** - By default, files are restored to their original location. To restore files to a different location, click **Choose location**. Each time files are automatically restored, they will be put in this configured location.

**Backup Settings**

Anti-Ransomware automatically backs up files before they are affected by a Ransomware attack. You can add files, processes, and certificates to the exclusion list to exclude them from backups.

• **Anti-Ransomware Maximum backup size on disk** - Set the maximum amount of storage for Anti-Ransomware backups. Best practice is to allow 1 GB.

• **Backup Time Interval** - Within this time interval, each file is only backed up one time, even if it is changed multiple times.

• **Change default file types to be backed up** - Click this to see a list of file types that are included in the Anti-Ransomware backup files. You can add or remove file types from the list and change the **Maximum Size** of files that are backed up.

**To add exclusions from Anti-Ransomware backups:**

1. From a SandBlast Agent Forensics and Anti-Ransomware rule in the Policy, right-click the Anti-Ransomware Backup Settings action and select **Edit Shared Action**.

2. Click **Add exclusion**.

3. In the window that opens select **Folder**, **Process**, or **Certificate**.

• **Folder** - To exclude all files in a folder, enter the Folder Name or browse to it.
• Optional: Select Include all sub folders to exclude all files contained in all sub folders.

• Process - To exclude an executable. You can also include Certificate information.
  ▪ In Process name, enter the name of the executable.
  ▪ Optional: Enter more information in the fields shown Signer is the company that signs the certificate. The more information you enter, the more specified the exclusion will be.

• Certificate - To exclude processes based on the company that signs the certificate, for example, Google.
  ▪ In Certificate Data, enter a name of company that signs certificates, or browse to add a certificate file.

4. Click OK.
5. The exclusion is added to the Exclusions list.

**Manual Anti-Ransomware Restoration**

If you select Automatic restore and remediate in the Anti-Ransomware Backup Settings Action, Anti-Ransomware automatically starts remediation after a Ransomware attack.

If you do NOT select Automatic restore and remediate, end-users must start restoration manually on the client computer after a Ransomware attack.

Best practice is to guide users through the process and instruct them what to select when there is more than one option.

**Anti-Ransomware Restoration**

In the SandBlast Agent Forensics Analysis Report (on page 195), you can see details of which files restored and deleted during the restoration.

• See which files were restored in the Business Impact section.
• See which files were deleted in the Remediation section.

**To run Anti-Ransomware restoration from a client computer:**

1. Right-click the Endpoint Security icon in the taskbar notification area and select Display Overview.
   The Endpoint Security Main Page opens.

2. Click the Forensics and Anti-Ransomware blade.

3. In the Analyzed cases table, click Restore Files in the row of the relevant incident.
   The Anti-Ransomware Restoration windows open.

4. Click Restore to start the restoration process.
   If you see a note that the files were already restored, click Cancel. It is not necessary to restore the files again.

5. In the Restore Step 1 of 2 window:
   a) Select the location to place the restored files:
      ▪ Restore files to the original location (default)
      ▪ Restore to selected location - If you select this, you are prompted to select the location.
   b) Delete files created by the attack, including encrypted files - This is selected by default.
      Clear it if you do not want to delete the files.
c) Click **Next**.

6. In the **Restore Step 2 of 2** window, click **Restore** to start the process. The Endpoint Security Restoration window opens and shows the files that were restored and where they are located.

7. Click **Close**.

### Integration with Third Party Anti-Virus Vendors

Forensics can use information from the Windows Event Log to monitor and analyze malware events from third party anti-virus vendors. Based on the Windows Event Log, Forensics can analyze attacks, terminate processes, delete or quarantine files, and do other attack remediation.

You can enable or disable third party integration in SmartEndpoint, from the **Automatic Threat Analysis** action. This works with most common vendors without manual configuration.

**Note** - Some third party vendors do not automatically send information to the Windows Event Log. To use third party vendor integration, make sure that your vendor is configured to send information to the Windows Event Log.

Events are detected when the client is online or offline.

**To enable or disable Forensics Third Party Anti-Virus Vendor integration:**

1. In a SandBlast Agent Forensics and Remediation rule, right-click the **Automatic Threat Analysis** Action and select **Edit Shared Action**.
2. In the bottom of the window, click **Override confidence level per specific event**.
   - The **Confidence level for automatic response** window opens.
3. In the **Additional Events** area, in the **Third party** row under **Forensics Analysis** -
   - Select **Always** to enable Third Party Anti-Virus Vendor integration.
   - Select **Never** to disable it.
4. Click **OK**.

### Manual Analysis with CLI

You can configure the Forensics blade to analyze incidents that are detected by a third party Anti-Malware solution. To use this, after an incident is triggered you can run analysis manually on the client computer or use a dedicated tool.

**To run analysis manually on a client computer with CLI:**

Use the command:
```
C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe
<Type>\Malicious resource>  [options]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Type&gt;</code></td>
<td>The type of <code>&lt;malicious&gt;</code>: URL, File, MD5, IP [Mandatory]</td>
</tr>
<tr>
<td><code>&lt;Malicious&gt;</code></td>
<td>The resource description (for example URL). [Mandatory]</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>- File description can be full path or just file name.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r, -remediation</td>
<td>Remediate malicious, suspicious, unknown processes based on policy configuration. [Optional]</td>
</tr>
<tr>
<td>-q, -quarantine</td>
<td>Enter the machine to restricted mode based on policy configuration. [Optional]</td>
</tr>
<tr>
<td>-id {GUID}</td>
<td>Set ID to incident. The format of the id is GUID. [Optional]</td>
</tr>
<tr>
<td>-b, -backup {Directory}</td>
<td>Backup Forensics Database to local file. [Optional]</td>
</tr>
<tr>
<td>-h, -help</td>
<td>Open help manual. [Optional]</td>
</tr>
</tbody>
</table>

#### Examples:

1. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe file:c:\test\test.doc url:www.test.com -r`
2. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe file:test.doc -r -q`
3. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe ip:170.12.1.180 file:test.doc`
4. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe HYPERLINK "url:www.Malicious.com" md5:10010010010010010010010010010010 -q -b c:\backupToFile.txt`
5. `C:\Program Files (x86)\CheckPoint\Endpoint Security\EFR\cpefrcli.exe -b c:\backupToFile.txt`

#### Notes:

1. All combination between optional parameters are allowed, the order is not important.
2. Backup option does not require Mandatory parameters (example 5).

### Manual Analysis with Push Operations

You can trigger incident analysis for a client on a one-time basis with Push Operations. You can run the Push Operation from SmartEndpoint or from the CLI. The analysis occurs without the need to install policy.

**To use Forensics Push Operations from SmartEndpoint:**

1. In SmartEndpoint, right-click on a computer object and select **Forensics**.
2. Select an option:
   - **Analyze by URL** - Enter the URL to inspect.
     - Optional - Enter data to search for an incident that occurred.
   - **Analyze by process or file** - Enter the full path to the file.
     - Optional - Enter data to search for an incident that occurred.
3. Click **OK**.
   The Forensics analysis runs on the users’ computer.
To use Forensics Push Operations from the Endpoint Security Management Server CLI:

For complete information about a dedicated tool and integration with third party Anti-Malware solutions, see sk105122 http://supportcontent.checkpoint.com/solutions?id=sk105122.

Run the $UEPMDIR/system/utils/EfrPushOperation.sh script on a computer, OU, or group.

Usage:

EfrPushOperation -name node_name|-fqdn node_FQDN|-dn node_DN -url URL|-file file [-i start_time [-r range]] [-a activity_event] [-c case_analysis_event] -u <username> -p <password>

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-name &lt;node_name&gt;</td>
<td>The requested node name as appears in SmartEndpoint</td>
</tr>
<tr>
<td>-fqdn &lt;node_FQDN&gt;</td>
<td>The requested node FQDN name, for example, <a href="mailto:device1@mycompany.com">device1@mycompany.com</a></td>
</tr>
<tr>
<td>-dn &lt;node_DN&gt;</td>
<td>The requested node distinguished name, for example, CN=device1,OU=Computers,DC=mycompany,DC=com</td>
</tr>
<tr>
<td>-url &lt;URL&gt;</td>
<td>Analyze by URL</td>
</tr>
<tr>
<td>-file &lt;file&gt;</td>
<td>Analyze by file or process</td>
</tr>
<tr>
<td>-i &lt;start_time&gt;</td>
<td>Incident start time (date and time)</td>
</tr>
<tr>
<td>-r &lt;range&gt;</td>
<td>Time range (before and after start time) in minutes</td>
</tr>
<tr>
<td>-a &lt;activity_event&gt;</td>
<td>'f' if detailed activity logs should not be generated, default is 't'</td>
</tr>
<tr>
<td>-c &lt;case_analysis_event&gt;</td>
<td>'f' if case analysis report should not be generated, default is 't'</td>
</tr>
<tr>
<td>-u &lt;username&gt;</td>
<td>Security Management Server username (case-sensitive)</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>Security Management Server password (case-sensitive)</td>
</tr>
</tbody>
</table>

SandBlast Agent Forensics Analysis Report

The SandBlast Agent Forensics Analysis Report provides full information on attacks and suspicious behavior with an easy interface. The report includes:

- **Entry Point** - How did the suspicious file enter your system?
- **Business Impact** - Which files were affected and what was done to them?
- **Remediation** - Which files were treated and what is their status?
- **Suspicious Activity** - What unusual behavior occurred that is a result of the attack?
- **Incident Details** - A complete visual picture of the paths of the attack in your system.
Use the Forensics Analysis Report to prevent future attacks and to make sure that all affected files and processes work correctly.

Opening Forensics Analysis Reports

The Forensics Analysis Report opens in your internet browser.

To open a Forensics Analysis Report for an incident:

- **SmartLog** - From the Log Details of a Forensics, Threat Emulation, or Anti-Bot log, under Forensics, click Report.
- **SmartEvent** - From the Summary of a Forensics, Threat Emulation, or Anti-Bot log, under Actions, click Open Forensics Report.
- **Endpoint Security Client GUI** - From the Client Overview, open the Forensics blade and click the Incident ID in the incident table.

SandBlast Agent Dynamic Updates

SandBlast Agent dynamic updates enable stronger security for endpoints, with regular updates to SandBlast Agent files. This keeps clients protected from the latest threats.

By default, the Threat Emulation blade runs the `EPNetUpdate.exe` process every 6 hours to get updates and update relevant files.

If necessary, you can disable the dynamic updates in GuiDBedit Tool.

To enable or disable SandBlast Agent dynamic updates:

1. Close all SmartConsole windows.
3. Search for `enable_efr_updatability`.
4. Change the value:
   - `true` - enabled (default)
   - `false` - disabled
5. Save the changes.
6. Close GuiDBedit Tool.
7. In SmartEndpoint, install policy.

SandBlast Agent Use Case

Scenario: You see a Threat Emulation or Anti-Bot detection log. What can you do?

Recommendations:

1. From the Forensics, Threat Emulation, or Anti-Bot log, open the Forensics Analysis Report.
2. Open the Remediation tab to see the components of the attack and how they were treated.
3. Delete all files that were created by the attack.
4. Open the Business Impact tab to see files that might be affected.
5. Open the **Entry Point** tab to see the path of the attack. Update your security policy to prevent similar attacks in the future.

### Ransomware Use Case

**Scenario:** A client computer is attacked by Ransomware. What can you do?

**Recommendations:**

1. From the Forensics log, open the Forensics Analysis Report.
2. Open the **Remediation** tab to see the components of the attack and how they were treated.
3. If **Automatic restore and remediate** is selected in the **Anti-Ransomware Backup Settings**, restoration and remediation was triggered and occurs automatically
   - If **Automatic restore and remediate** is **NOT** selected in the **Anti-Ransomware Backup Settings**, instruct the user to run the Anti-Ransomware Restoration manually from the client computer (on page 192).
4. Analyze the Forensics Analysis Report and update your security policy to prevent similar attacks in the future.

### Quarantine Management

When SandBlast Agent blades (Forensics and Anti-Ransomware, Anti-Bot, and Threat Extraction and Threat Emulation), detect malicious files, they can quarantine those files automatically based on policy. All blades use the same remediation service, that:

- Receives the request to quarantine a file.
- Terminates the file’s process, if running.
- Encrypts the file and stores it compressed along with metadata in a protected folder.

Two utilities let administrators and end-users manage quarantined files.

**SandBlast Agent Quarantine Manager**

The **SandBlast Agent Quarantine Manager** utility is called **RemediationManagerUI.exe** and it is located in `C:\Program Files (x86)\CheckPoint\Endpoint Security\Remediation` on client computers. It lets end-users:

- See the files in quarantine
- Delete the quarantined files
- Restore files from quarantine.

**SandBlast Agent Quarantine Manager for Administrators**

The administrator utility contains the capabilities of the end-user utility plus these additional features:

- **Quarantine** - Send files to quarantine.
- **Delete** - Use the SandBlast Agent remediation service to delete a file.
- **Import** - Import a quarantined file from a different computer or location.
Get the administrator utility from the release homepage [http://supportcontent.checkpoint.com/solutions?id=sk115512].

**Using the Quarantine Manager for Administrators**

When you open the SandBlast Agent Quarantine Manager or the SandBlast Agent Quarantine Manager for Administrators, each quarantined item is shown as a file. The name of the file is the incident ID. To find a file, search for the incident ID found in the SandBlast Agent logs.

By default, quarantined files stored on the client are in C:\ProgramData\CheckPoint\Endpoint Security\Remediation\quarantine on the client computer.

Best practice is to configure Copy quarantine files to a central location in the File Quarantine Settings [on page 190]. Then you can use the Quarantine Manager for Administrators to import all files related to an incident from one location that you can access.

From the Quarantine Manager for Administrators you can:

- Restore files in a protected location to test them.
- Collect all malicious files related to an attack for research.

To permanently delete an item:

1. Open the SandBlast Agent Quarantine Manager for Administrators.
2. Select one or more items.
3. Click **Delete**.

To send a file to quarantine from outside of the utility:

1. Open the SandBlast Agent Quarantine Manager for Administrators.
2. Click **Quarantine**.
3. In the window that opens, browse to select the file to move to quarantine.

To import a suspicious file to the utility:

1. Open the SandBlast Agent Quarantine Manager for Administrators.
2. Click **Import**.
3. In the window that opens, browse to select the quarantined file to import.

   The file, with its metadata, is imported to the quarantine database from where the utility is run.
SandBlast Agent Anti-Bot

In This Section:

The Need for Anti-Bot .........................................................................................................199
The SandBlast Agent Anti-Bot Solution ..............................................................................200
Configuring Anti-Bot Policy Rules .....................................................................................200

The SandBlast Agent Anti-Bot Software Blade monitors endpoint computers for bot-related communication and alerts administrators about devices affected by bot activity.

Configure the settings in the SandBlast Agent Anti-Bot rule of in the SmartEndpoint Policy tab.

The Need for Anti-Bot

There are two emerging trends in today's threat landscape:

- A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.

- Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.

Both of these trends are driven by bot attacks.

A bot is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.

When a bot infects a computer, it:

- Takes control over the computer and neutralizes its Anti-Virus defenses. Bots are difficult to detect since they hide within your computer and change the way they appear to Anti-Virus software.

- Connects to a Command and Control (C&C) center for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to execute illegal activities without your knowledge. These activities include:
  - Data theft (personal, financial, intellectual property, organizational)
  - Sending SPAM
  - Attacking resources (Denial of Service Attacks)
  - Bandwidth consumption that affects productivity

In many cases, a single bot can create multiple threats. Bots are often used as tools in attacks known as Advanced Persistent Threats (APTs) where cyber criminals pinpoint individuals or organizations for attack. A botnet is a collection of compromised computers.

Check Point's Endpoint Anti-Bot Software Blade detects and prevents these bot threats.
The SandBlast Agent Anti-Bot Solution

The Anti-Bot Software Blade:

• Uses the ThreatCloud repository to receive updates and queries it for classification of unidentified IP, URL, and DNS resources.
• Prevents damage by blocking bot communication to C&C sites and makes sure that no sensitive information is stolen or sent out of the organization.

The Endpoint Anti-Bot blade uses these procedures to identify bot infected computers:

• Identify the C&C addresses used by criminals to control bots
• These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

Check Point uses the ThreatCloud repository to find bots based on these procedures.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Endpoint Anti-Bot blade gets reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified URL/DNS resources that it finds.

Configuring Anti-Bot Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select New to define a custom Action option.

Right-click an Action and select Edit or Edit Shared Action to change the Action behavior.

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

Blade Activation

Define the prevention and detection settings for the Anti-Bot blade. The automatic options are:

• Prevents high confidence bots, detects all - All bots are detected and logged. Anti-Bot only blocks activity when it is almost certain that the activity is malicious (high confidence). This is the default.
• Anti-bot detection is enabled - All bots are detected and logged but not blocked.
• Anti-bot is not active - Client computers are not monitored for bot activity.

The confidence level is how sure Endpoint Security is that activity is malicious. High confidence means that it is almost certain that the activity is malicious. Medium confidence means that it is very likely that the activity is malicious.

In the Blade Activation action, you can manually change the settings for each confidence level.

Select actions for High Confidence, Medium Confidence, and Low Confidence bots:

• Prevent - Blocks bots.
• Detect - Logs information about bots, but does not block them.
• Inactive - Ignores bots (does not prevent or detect them).
Detection Exclusions

By default, the Anti-Bot Software Blade inspects all domains.

You can configure trusted entities, which will not be inspected by the Anti-Bot Software Blade.

To configure detection exclusions:

1. In the Properties of the Detection Exclusions Action, select an option from the Select action drop-down menu.
   To create a new action profile, click New, and in the window that opens enter the name and the description and Click OK.
2. Select Allow detection exclusions for following trusted entities.
3. Click Add exclusion.
4. In the window that opens, select the Object Type, click OK, and enter the name of the new exclusion:
   - **Process** - Name of an executable
   - **URL** - Website URL
   - **Domain** - Full domain name
   - **Protection Name** - Predefined malware signature
   - **IP Range** - Internal or External IP addresses
5. Click OK.
6. Click OK.

Anti-Bot Protection Mode

By default, the Anti-Bot Default protection mode allows connections while it checks for bots in the background. You can choose to block connections until the threat check is complete.

To configure General Settings:

1. In the Properties of the General Settings Action, select an option from the Select action drop-down menu.
   To create a new action profile, click New, and in the window that opens enter the name and the description and Click OK.
2. Select the default behavior:
   - **Background** - connections are allowed until threat check is complete
   - **Hold** - connections are blocked until threat check is complete
3. **Hours to suppress logs for same bot protection** - To minimize the size of the Anti-Bot logs, actions for the same bot are only logged one time per hour. To change the default log interval, select a number of hours.
4. **Days to remove bot reporting after** - If a bot does not connect to its command and control server after the selected number of days, the client stops reporting that it is infected.
5. Click OK.
Overview of SandBlast Agent Threat Extraction and Threat Emulation

Threat Emulation detects zero-day and unknown attacks. Files on the endpoint computer are sent to a sandbox for emulation to detect evasive zero-day attacks.

Threat Extraction proactively protects users from malicious content. It quickly delivers safe files while the original files are inspected for potential threats.

As part of the Threat Extraction and Threat Emulation solution, when the SandBlast Agent client is installed on a client computer, the SandBlast Agent Browser Extension is also installed on the Google Chrome browser. The SandBlast Agent Browser Extension protects against malicious files that come from internet sources.

See all Threat Extraction and Threat Emulation logs in SmartLog under Threat Emulation.

- Logs related to files from the SandBlast Agent Browser Extension show: **Monitor Type - Browser Extension** and **Browser - Chrome**
- Logs related to files from the computer show: **Monitor Type - File Monitor**

Configure the settings in the **SandBlast Agent Threat Extraction and Threat Emulation** rule of in the SmartEndpoint **Policy** tab.

Configuring Threat Extraction and Threat Emulation Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

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

Define the settings for the SandBlast Agent Browser Extension to protect against malicious files that come from internet sources. The Browser Extension is supported on Google Chrome.

The automatic options are:

- **Protect web downloads with Threat Extraction and Emulation** - Send files for emulation. While a file is tested, users receive a copy of it with all suspicious parts removed. If the file is not malicious, users receive the original file when the emulation is finished. Emulation can take up to two minutes.

- **Protect web downloads with Threat Emulation** - Send files for emulation. Users do not receive a copy during the emulation. If the file is not malicious, users receive the original file when the emulation is finished. Emulation can take up to two minutes.

- **Do not use web download protection** - The SandBlast Agent Browser Extension is not active.

When Threat Extraction is selected, it only applies to file types that can be extracted, such as documents.

When Threat Emulation is selected, it only applies to file types that can be emulated, such as executables and scripts.

You can edit the selections manually to define more settings for Threat Extraction and Threat Emulation for different file types.

**To change the setting for categories of file types:**

1. In a SandBlast Agent Threat Extraction and Threat Emulation rule, right-click the **Web Download Protection** Action and select **Edit Shared Action**.
2. Expand the list for the type of file that you choose:
   - **Files that can be extracted and emulated** (such as documents and pictures).
   - **Files that can only be emulated** (such as executables and scripts).
   - **When neither Extraction nor Emulation is supported** (such as videos).
3. Select an option for emulation and access to the original file from the options shown. Different options show for different file types.
   - **Extract and suspend original file until emulation completes** - Send files for emulation. While a file is tested, the user receives a copy of it with all suspicious parts removed.
   - **Emulate and suspend original file until emulation completes** - Send files for emulation. Users only receive the files after the emulation finishes and the file was found to be safe.
   - **Emulate original file without suspending access** - Send files for emulation. Users can download and access the file while it is tested. The administrator is notified if files are found to be malicious.
   - **Allow Download** - No emulation or extraction. The download is allowed.
   - **Block Download** - No emulation or extraction. The download is blocked.
4. If files are extracted, select the **Extract Mode**, which is the format of the extracted document that users can see during the emulation.
   - **Extract potentially malicious elements** - The file is sent in its original file type but without malicious elements.
   - **Convert to PDF** - When relevant, files are converted to PDF.
5. Click **OK**.
To change the setting for a specified file type, such as .zip or .pdf:

1. In a SandBlast Agent Threat Extraction and Threat Emulation rule, right-click the Web Download Protection Action and select Edit Shared Action.
2. Click Override default file action per file type.
3. Select a file type.
4. Click in the File Action column to select a different action for that file type.
5. Click in the Extraction Mode column to select a different extraction mode for the file type.
6. Click OK.

**File System Emulation**

Define the default settings for emulation of files on the file system. The automatic options are:

- **Emulate files written to file system** - All files that can be emulated are automatically sent for emulation when they are written to the file system.
- **Do not emulate files written to file system** - Files are not automatically sent for emulation when they are written to the file system.

Monitoring is enabled by default for all options.

**SandBlast Environment Settings**

By default, SandBlast Agent uses the SandBlast Cloud for Threat Extraction and Threat Emulation. If you have one or more SandBlast Appliances, you can use them as an alternative to SandBlast Cloud.

To configure SandBlast Agent to work with a SandBlast Appliance:

1. In a SandBlast Agent Threat Extraction and Threat Emulation rule, right-click the SandBlast Environment Settings Action and select Edit Shared Action.
2. Select Use SandBlast Appliance for Threat Extraction and Threat Emulation.
3. In the Properties of the action, click Configure Appliances.
4. In the Appliances Configuration window, select an appliance from the list, or click Add and enter:
   - **IP address** of the SandBlast Appliance
   - **Appliance Certificate Name** - Click Manage to select a certificate or to import one.
5. To configure a certificate for communication between SandBlast Agent and the SandBlast Appliance, see sk116381 [http://supportcontent.checkpoint.com/solutions?id=sk116381](http://supportcontent.checkpoint.com/solutions?id=sk116381).
6. By default the Cloud will be used if the Appliance is not available. If you do not want the SandBlast Cloud to be used as backup, clear the option If appliance is not available, fallback to Cloud.
7. Click OK.
To define the maximum size of files that are sent for emulation:

1. In a SandBlast Agent Threat Extraction and Threat Emulation rule, right-click the SandBlast Environment Settings Action and select Edit Shared Action.
2. Change the value for Upload to emulation files less than X Megabytes. The default is that file less than 10 MB are sent for emulation.

Configuring Multiple SandBlast Appliances

SandBlast Agent can work with multiple SandBlast appliances for load sharing and redundancy.

You can configure load sharing in these ways:

- If your environment has a Security Gateway for Threat Prevention load sharing, add this gateway as an appliance for SandBlast Agent and it will do the load balancing transparently. See sk102309 http://supportcontent.checkpoint.com/solutions?id=sk102309 for more details about Security Gateway configuration with multiple Threat Emulation Private Cloud Appliances.
- In a SandBlast Agent Threat Extraction and Threat Emulation rule > SandBlast Environment Settings, add the appliances. Each SandBlast Agent client does the load sharing. Each client builds a list of appliances, sorts it randomly, and then uses the first appliance from that list. If an appliance becomes unavailable, it is removed from the list and added later to the end of the list.

Exclusions and Inspection Settings

The default behavior is Inspect all domains and files. All files in the file system are inspected and sent for emulation when applicable. You can configure exclusions that are not inspected.

Click Add exclusion to exclude a file or process from inspection. You can define an exclusion by many different criteria. Criteria include: Domain, folder, and SHA1 hash. Add more information to make the exclusion very specific and less information to make it broad.

Notes on exclusions:

- Domain exclusions are not supported by file system emulation.
- SHA1 exclusions are not supported by the SandBlast Agent Browser Extension.
- When you exclude a folder, enter the folder as a Windows path, for example: C:\Windows\System32\user\.
- Folder exclusions support wildcards. These wildcards are supported:
  - ? -- Each question mark masks one character
  - * -- Each star masks zero or more characters

Zero Phishing Settings

Define setting for phishing prevention and password reuse prevention.

- **Phishing Prevention** - Checks different characteristics of a website to make sure that a site does not pretend to be a different site and use personal information maliciously.
- **Password Reuse Prevention** - Alerts users not to use their corporate password in non-corporate domains.
Phishing Prevention

- **Phishing Protection** - Select an option:
  - **Prevent Access and Log** (default) - If SandBlast Agent determines that the site is phishing, users cannot access the site. A log is created for each malicious site.
  - **Off** - Phishing prevention is disabled.
  - **Log Only** - When a user uses a malicious site, a log is created.
  - **Prevent Access Only** - Users cannot access malicious sites. No logs are created.

- **Send log on each scanned site** - Send logs for each site that users visit, if it is malicious or not.

- **Allow user to dismiss the phishing alert and continue to access the site** - Users can choose to use a site that was found to be malicious.

- **Allow user to abort phishing scans** - Users can stop the phishing scan before it is completed.

Password Reuse

- **Password Reuse Protection** - Select an option:
  - **Alert User and Log** (default) - If a user enters a corporate passwords in a non-corporate site, the user gets an alert and a log is created.
  - **Off** - Password Reuse Prevention is disabled.
  - **Log Only** - If a user enters a corporate passwords in a non-corporate site, a log is created.
  - **Alert User Only** - If a user enters a corporate passwords in a non-corporate site, the user gets an alert.

- **Protected Domains** - Add domains for which Password Reuse Protection is enforced. SandBlast Agent keeps a cryptographic secure hash of the passwords used in these domains and compares them to passwords entered outside of the protected domains.
Compliance

In This Section:

- Overview of Compliance .................................................................207
- Planning for Compliance Rules .......................................................207
- Configuring Compliance Policy Rules ............................................208
- Monitoring Compliance States ........................................................213
- The Heartbeat Interval ....................................................................214

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 (on page 71).

Planning for Compliance Rules

Before you define and assign compliance rules, do these planning steps:

1. Identify the applications, files, registry keys, and process names that are required or not permitted on endpoint computers.

2. Collect all information and remediation files necessary for user compliance. Use this information when you create remediation objects to use in compliance rules.

Compliance rules can prevent users from accessing required network resources when they are not compliant. Think about how to make it easy for users to become compliant.
3. Make sure that the firewall rules gives access to remediation resources. For example, sites from which service packs or Anti-virus updates can be downloaded.

   **Note** - In Windows 7, make sure the **Interactive Service Detection** service is running. This is necessary for remediation files (running with system credentials) that must interact with the user.

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

### Configuring Compliance Policy Rules

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select **New** to define a custom Action option.

Right-click an Action and select **Edit** or **Edit Shared Action** to change the Action behavior.

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

#### 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.
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><strong>Observe</strong></td>
<td>Log endpoint activity without further action. Users do not know that they are non-compliant. Non-compliant endpoints show in the <strong>Observe</strong> state in the <strong>Reporting</strong> tab.</td>
</tr>
<tr>
<td><strong>Warn</strong></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><strong>Restrict</strong></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 <strong>about to be restricted</strong> state. On the monitoring tab, the user is shown as <strong>pre-restricted</strong>.</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 (on page 209).
   c) Select an **Action** from the list.
   d) Click the **Remediation** tab to add remediation objects to the rule (on page 211). 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>
<tr>
<td>Check Registry</td>
<td>Select one of these options to enable the registry check or clear to disable it:</td>
</tr>
<tr>
<td>Registry key and value exist</td>
<td>Find the registry key and value. If the registry key exists, the endpoint computer is compliant for the required file.</td>
</tr>
<tr>
<td>Registry key and value do not exist</td>
<td>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.</td>
</tr>
<tr>
<td>Registry Key</td>
<td>Enter the registry key.</td>
</tr>
<tr>
<td>Registry Value</td>
<td>Enter the registry value to match.</td>
</tr>
<tr>
<td>Check File</td>
<td>Select one of these options to check if an application is running or if a file exists:</td>
</tr>
<tr>
<td>File is running at all times</td>
<td>For example, make sure that Endpoint Security client is always running.</td>
</tr>
<tr>
<td>File exists</td>
<td>For example, make sure that the user browsing history is always kept.</td>
</tr>
<tr>
<td>File is not running</td>
<td>For example, make sure that DivX is not used.</td>
</tr>
<tr>
<td>File does not exist</td>
<td>For example, make sure that a faulty DLL file is removed.</td>
</tr>
<tr>
<td>File Name</td>
<td>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).</td>
</tr>
<tr>
<td>File Path</td>
<td>Enter the path without the file name. Select the <strong>Use environment Variables of logged in user</strong> option to include paths defined in the system and user variables. Do not add the &quot;&quot; character at the end of the path.</td>
</tr>
<tr>
<td>Check File Properties</td>
<td>Additional options to check for an existing or non-existing file.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Match File Version</td>
<td>Make sure that a specific version or range of versions of the file or</td>
</tr>
<tr>
<td></td>
<td>application complies with the file check.</td>
</tr>
<tr>
<td>Match MD5 Checksum</td>
<td>Find the file by the MD5 Checksum. Click <strong>Calculate</strong> to compare the</td>
</tr>
<tr>
<td></td>
<td>checksum on the endpoint with the checksum on the server.</td>
</tr>
<tr>
<td>File is not older than</td>
<td>Select this option and enter the maximum age, in days, of the target file.</td>
</tr>
<tr>
<td></td>
<td>If the age is greater than the maximum age, the computer is considered</td>
</tr>
<tr>
<td></td>
<td>to be compliant. This parameter can help detect recently installed,</td>
</tr>
<tr>
<td></td>
<td>malicious files that are disguised as legitimate files.</td>
</tr>
</tbody>
</table>

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</td>
</tr>
<tr>
<td></td>
<td>compliant.</td>
</tr>
<tr>
<td>Download Path</td>
<td>• Enter the temporary directory on the local computer to download the</td>
</tr>
<tr>
<td></td>
<td>program or script to. This path must be a full path that includes the</td>
</tr>
<tr>
<td></td>
<td>actual file and extension (*.bat or *.exe).</td>
</tr>
<tr>
<td></td>
<td>• This parameter is required.</td>
</tr>
<tr>
<td></td>
<td>• The endpoint client first tries to access the file from the specified</td>
</tr>
<tr>
<td></td>
<td>path. If the client fails, it downloads the file from the URL to the</td>
</tr>
<tr>
<td></td>
<td>temporary directory and runs it from there.</td>
</tr>
<tr>
<td></td>
<td>• To run multiple files, use one of the popular compression programs</td>
</tr>
<tr>
<td></td>
<td>such as <strong>WinRAR</strong> to produce a self-extracting executable that contains a</td>
</tr>
<tr>
<td></td>
<td>number of .exe or .bat files.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **URL**                 | • Enter the URL of an HTTP or file share server where the file is located.  
• Enter the full path that includes the actual file with one of the supported extensions (*.bat or *.exe).  
• This field can be left empty.  
• Make sure the file share is not protected by a username or password. |
| **Parameters**          | If the executable specified in the URL runs an installation process, make sure that the executable holds a parameter that specifies the directory where the program should be installed. If the executable does not hold such a parameter, enter one here. |
| **MD5 Checksum**        | Click **Calculate** to generate a MD5 Checksum, a compact digital fingerprint for the installed application or the remediation files.        |
| **Run as System**       | Apply system rights for running the executable file. Not all processes can run with user rights. System rights may be required to repair registry problems and uninstall certain programs. |
| **Run as User**         | Apply user rights and local environment variables for running the executable file.                                                             |
| **Messages**            |                                                                                                                                              |
| **Automatically**       | Run the executable file without displaying a message on the endpoint computer.                                                              |
| **execute operation**   | Run the executable file only after a user message opens and the user approves the remediation action. This occurs when **Warn** or **Restrict** is the selected action on a compliance check. |
| **without user**        |                                                                                                                                              |
| **notification**        |                                                                                                                                              |
| **Execute operation**   | Run the executable file only after a user message opens and the user approves the remediation action. This occurs when **Warn** or **Restrict** is the selected action on a compliance check. |
| **only after user**     |                                                                                                                                              |
| **notification**        |                                                                                                                                              |
| **Use same message**    | Select that the same text be used for both messages.                                                                                                                                                   |
| **for both**            | A Non-Compliant message tells the user that the computer is not complaint and shows details of how to become compliant.                                                                             |
| **Non-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. |
| **and Restricted**      |                                                                                                                                              |
| **messages**            |                                                                                                                                              |
| **Message Box**         | Displays selected non-compliant and restricted messages. The message box is available only by selecting the Execute only after user notification setting. Click **Add**, **Remove**, or **Edit** to add a message, and remove or revise a selected message. |
| **Note**                | **Note**: User cannot prevent the remediation application or file from running.                                                                |
Service Packs for Compliance

The Service Packs Compliance Action makes sure that computers have the most recent operating system service packs and updates installed. The default settings show in the Latest Service Packs Installed Action Rules.

See Compliance Action Rules (on page 209) for more information.

Required Applications and Files

Required Application and File Compliance Settings look for the presence of specified files, registry values, and processes that must be running or present on endpoint computers. The default settings show in the Required Application Action Rules.

For Required Application action rules, multiple check objects in the rule are mutually exclusive. If one or more check object is not compliant, the defined action and remediation is triggered.

See Compliance Action Rules (on page 209) 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 209) for more information.

Anti-Malware for Compliance

The Anti-Malware check makes sure that computers have an anti-malware program installed and updated. The default settings show in the Anti-Malware Compliance Action Rules.

See Compliance Action Rules (on page 209) for more information.

Monitoring Compliance States

Monitor the compliance state of computers in your environment from:

- SmartView Tracker
- The Security Overview
- Reporting > Compliance

These compliance states are used in the Security Overview and Compliance reports:

- **Compliant** - The computer meets all compliance requirements.
- **About to be restricted** - The computer is not compliant and will be restricted if steps are not done to make it compliant. See Configuring the "About to be Restricted" State (on page 72).
- **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 > Endpoint Connection Settings.
   - The **Connection Settings 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. Click Manage > Endpoint Connection Settings.
   - The **Connection Settings Properties** window opens.
2. In the **Out of Compliance** section, enter the number of heartbeats.
3. Click **OK**.

When you configure this time period, we recommend that you give users sufficient opportunity to:

• Save their data.
• Correct the compliance issues.
• Make sure that the endpoint computer is compliant.

The formula for converting the specified time period to minutes is:

\[
\text{<number of heartbeats> } \times \text{<heartbeat interval (in seconds)> } \times 60.
\]
Firewall

In This Section:

- Planning Firewall Policy ................................................................. 215
- Inbound Traffic Rules ..................................................................... 215
- Outbound Traffic Rules .................................................................. 216
- Creating Firewall Rules ................................................................. 216
- Wireless Connection Settings ......................................................... 218
- Hotspot Settings ............................................................................ 218
- IPv6 Traffic .................................................................................. 219
- Choose a Firewall Policy to Enforce ............................................... 219

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</td>
<td>Allows all incoming traffic from trusted zones and IP obtaining traffic from the internet. All other traffic is blocked.</td>
</tr>
<tr>
<td>and connectivity services</td>
<td></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>NO</td>
<td>Rule priority number. Rule priority is important because a client checks firewall rules based on its sequence in the Rule Base. Rules are enforced from the top to the bottom. The last rule is usually a Cleanup Rule that says to drop traffic that does not match any of the previous rules.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Firewall Rule.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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**.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Track                  | When the rule is enforced:  
• **Log** - Record rule enforcement in the Endpoint Client Log Viewer.  
• **Alert** - Show a message on the endpoint computer and record rule enforcement in the Endpoint Client Log Viewer.  
• **None** - Log and alert messages are not created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Notes on configuring Tracking:**

- If you have a rule that drops or accepts all traffic, do not enable logging.
- To use logs and alerts, you must configure options in the **Client Settings** rules:
  - In the **Log Upload** action, **Enable log upload** must be selected.
  - In the **Users Disabling Network Protection** action, under **Network Protection Alerts**, in the **Firewall** row, select **Allow Alert**.

**Firewall Rules and Domain Controllers**

⚠️ **Important** - When creating Firewall Rules for endpoint clients, create explicit rules that allow all endpoints to connect to all of the domain controllers on the network.

**Services and Network Objects**

The same Network Objects and Services are used throughout the SmartEndpoint and in 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.
Access Zones

In This Section:

- Trusted Zone ............................................................................................................... 220
- Changing the Access Zones Policy ............................................................................ 221
- Network Objects ......................................................................................................... 222

Access Zones lets you create security zones for use in Firewall. Configure Access Zones before configuring Firewall.

There are two predefined Access Zones:

- The **Internet Zone**
- The **Trusted Zone**

Network locations not placed in the **Trusted Zone** automatically belong to the **Internet Zone**.

**Note**: Access Zones rules are computer-centric (and not user-centric).

**Trusted Zone**

The Trusted Zone contains network objects that are trusted. Configure the Trusted Zone to include only those network objects with which your programs must interact.

*Note* - Objects not placed in the **Trusted Zone** are placed automatically in the **Internet Zone**.

SmartEndpoint contains an initial Access Zones policy. In the initial policy, these network elements are included in the Trusted Zone:

- **All_Internet**
  This object represents all legal IP addresses. In the initial policy, all IP addresses on the Internet are trusted. However, the Access Zones policy is not a policy that is enforced by itself but only as a component of the Firewall policy.

- **LocalMachine_Loopback**
  Endpoint computer’s loopback address: 127.0.0.1. The Endpoint must always have access to its own loopback address.

  *Note* - Endpoint users must not run software that changes or hides the local loopback address, for example personal proxies that enable anonymous internet surfing.

**Objects in the Trusted Zone**

Think about adding these objects to your Trusted Zone:

- Remote host computers accessed by your programs (if not included in the subnet definitions for the corporate network)
- Corporate WANs accessed by your programs
- Endpoint Security Management Server
- Domain name servers
- Mail servers
- Domain controllers
- File servers
- Print servers
- VPN 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.

You can add and remove network objects from a Trusted Zone.

*Note* - A computer can have only one Trusted Zone. This means that if the Access Zones policy has more than one rule, and more than one Trusted Zone applies to a computer, only the last Trusted Zone is enforced.

To define the Trusted Zone:

1. In the **Policy** tab > **Access Zones** rule, double click **Corporate Trusted Zones** or right-click it and select **Edit Shared Action**. The **Edit Properties - Access Zones** window opens.

2. To **add** an existing object to the **Trusted Zone Locations** list:
   - Select a network object from **Available Network Objects**.
   - Click **Add**.

3. To **remove** an existing object:
   - Select the network object from the list
   - Click the **Remove** arrow

4. To **delete** an existing object, select the object and click **Delete**.

5. To **create** a new Network Object, click **New**. The **Select New Object Type** window opens.
   a) Select an object type from the list.
   b) Click **OK**.
      - The **Properties** window for the selected object opens.
   c) Enter the required data.

6. Click **OK**.
To create a new Trusted Zone object:

1. In the Policy tab > Access Zones rule, double click Corporate Trusted Zones or right-click it and select Edit Properties.
   The Properties window opens.
2. In the Select action field, select New.
3. Edit the Name and Description of the Zone.
4. Click OK.
5. Edit the network locations in the zone as described in the procedure above.

Network Objects

Access Zones are made up of network objects. You define network objects by specifying one or more:
- Host
- IP address range
- Network
- Site

Create network objects for areas that programs must have access to, or areas that programs must be prevented from accessing.

Define objects for each policy or define objects before you create a policy. After defining an object, the object can be reused in other policies.

The same Network Objects and Services are used throughout the SmartEndpoint and in 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 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 23: Application Control

In This Section:
- Working with the Application Control Policy ............................................................. 225
- Reputation Service ...................................................................................................... 226

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:
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 common
applications and operating system files on endpoint computers network. This is especially useful
when you have a clean standard image.

You can 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 sk108536
   http://supportcontent.checkpoint.com/solutions?id=sk108536, to the root directory (typically
c:) of the baseline reference source computer.

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 string> /e /a /p /verbose /warnings /?]

Parameters

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

Examples
- appscan /o scan1.xml
  This scan, by default, includes .exe files in the current directory and is saved as scan1.xml.
• appscan /o scan2.xml /x ".exe;.dll" /s "C:\"
  This scan includes all .exe and .dll files on drive C and is saved as scan2.xml.

• appscan /o scan3.xml /x ".dll" /s c:\program files
  This scan included all .dll files in c:\program files and all its subdirectories. It is saved as scan3.xml.

• appscan /s "C:\program files" /e
  This scan includes all executable files in c:\program files and all its subdirectories. It is saved as the default file name scanfile.xml.

**Importing 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.
Client Settings

In This Section:
Configuring Client Settings Policy Rules ..........................................................230

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

Configuring Client Settings Policy Rules

The Client Settings Actions in the rules set:

- General user interface settings
- If users can postpone installations and for how long.
- The client uninstall password
- When log files are uploaded to the server
- Specified Network Protection settings

For each Action in a rule, select an option, which defines the Action behavior. You can select a predefined Action option or select New to define a custom Action option.

Right-click an Action and select Edit or Edit Shared Action to change the Action behavior.

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

Client User Interface Settings

You can choose the default client user interface settings or edit them to customize the Endpoint Security client interface on user computers.

You can change these settings:

- **Display client icon** - When selected, the client icon shows in the windows notification area when the Endpoint Security client is installed.

- **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>
</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>
</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 <strong>Disable Network Protection</strong> 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. You must also select this to use **Alert** in the **Track** column of Firewall rules.
Sharing Data with Check Point

Clients can share information about detected infections and bots with Check Point. The information goes to ThreatCloud, a Check Point database of security intelligence that is dynamically updated using a worldwide network of threat sensors. ThreatCloud helps to keep Check Point protection up to date with real-time information.

Note - Check Point does not share any private information with third parties.

To configure data ThreatCloud sharing:

1. In the Properties of the ThreatCloud Sharing Action, select an option from the Select action drop-down menu.
   To create a new action profile, click New, and in the window that opens enter the name and the description and Click OK.

2. Select or clear:
   - Enable sharing data with Check Point [default]
   - Disable sharing data with Check Point

3. Click OK.
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 E80.65**. For more information, see the E80.65 Endpoint Security and Remote Access VPN Clients homepage [http://supportcontent.checkpoint.com/solutions?id=sk115512](http://supportcontent.checkpoint.com/solutions?id=sk115512).
URL Filtering

For information about URL Filtering with Endpoint Security, the *URL Filtering with Endpoint Security Administration Guide*
Remote Help

In This Section:
- Overview of Remote Help ................................................................. 236
- Web Remote Help ............................................................................. 236
- Giving Remote Help to Full Disk Encryption Users ......................... 242
- Media Encryption & Port Protection Remote Help Workflow .......... 243
- Disabling Remote Help .................................................................... 244
- User-Bound Remote Help ................................................................. 244

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 applicable for users with fixed passwords who are locked out.
  For USB storage devices protected by Media Encryption & Port Protection policies, only remote password change is available.

Web Remote Help

Administrators can use the built in Remote Help or online portal on the Endpoint Security Management Server, or create a dedicated server for the online web portal.

A dedicated server for the online web portal is supported with E80.60 and higher management. It is supported on Gaia servers only.

If there is one or more external Remote Help Server in an environment, you must use online synchronization.
Administrators can authenticate to the web portal with these authentication methods:

- Check Point Password login (default) - Configure this in SmartEndpoint
- Active Directory Password - See Configuring SSL Support for AD Authentication
- Dynamic Token

### Turning on Web Remote Help on Endpoint Security Management Server

On E80.60 management and higher, you must turn on the Web Remote Help in SmartEndpoint before you can use it.

**To turn on the Web Remote Help:**

1. In SmartEndpoint, go to Manage > Endpoint Servers. The **Endpoint Server** window opens.
2. Double-click on the name of an existing server on the list.
3. Select **Remote Help Server**.
4. Click **Next**.
5. Install Database.

When you turn on or turn off the Web Remote Help, the Endpoint Security Management Server restarts and all connections with client computers and SmartEndpoint sessions get disconnected.

### Configuring the Length of the Remote Help Response

Administrators can configure how many characters are in the Remote Help response that users must enter. The default length is 30 characters.

This feature requires an E80.60 or higher Endpoint Security client.

**To change the length of the Remote Help response:**

1. In the **Policy tab**, **Full Disk Encryption** rule, double-click the **Pre-boot Protection** action.
2. In the **Pre-boot Protection Properties** window, click **Advanced Pre-boot Settings**.
3. In the **General Pre-boot Settings** window, **Remote Help** area, select a **Remote Help response length**.
4. Click **OK**.
5. Click **OK**.
6. Install policy.

### Logging into Web Remote Help portal

You can log into Web Remote Help portal using one of these methods:

- Password Login
- Token Login

Password Login is the default method and shows when you first connect to the portal. The link in the right bottom corner of the Endpoint Security Web Remote Help window lets you toggle between the two login methods.
To login using Password Login method:

1. Enter a User Name and select a domain name from the Domains list.
   
   Notes -
   - You can set the user name in UPN format, for example: 
     UserName@ExamapleCompany.com
   - Domain name for the internal users is internal-users

2. Enter the Password.
3. Click Log In.

To login using Token Login method:

1. Enter a User Name and select a domain name from the Domains list.
   
   Notes -
   - You can set the user name in UPN format, for example: 
     UserName@ExamapleCompany.com
   - Domain name for the internal users is internal-users

2. Click Next.
3. Enter the Challenge string into your token.
4. Enter the Response generated by the X.99 Token.
5. Click Login.

Configuring a Standalone Web Remote Help Server

On E80.60 and higher management, you can configure a standalone Web server for Remote Help. This is supported on Gaia servers only.

To configure a Standalone Remote Help Server:

1. In SmartEndpoint, go to Manage > Endpoint Servers.
   The Endpoint Server window opens.

2. Click New.
4. In the window that opens, select Endpoint Security Management Server.
5. Enter Server Name and IP Address.
6. Select a color (optional).
7. Enter a comment (optional).
8. Click Next.
9. Create SIC trust between the Primary Endpoint Security Management Server and the Remote Help sever:
   a) Enter the same SIC Activation Key as the one you entered in the Check Point Configuration Tool.
   b) Click Initialize to create a state of trust between the Endpoint Security Management Servers.
   c) If trust creation fails, click Test SIC Status to see troubleshooting instructions.
   d) If you have to reset the SIC, click Reset, reset the SIC on the Remote Help server, then click Initialize.
10. Install Database on all servers.

Managing Web Remote Help Accounts

You can do these web Remote Help account management actions:

- Add web Remote Help accounts
- Delete web Remote Help accounts
- Edit web Remote Help accounts
- Search for existing web Remote Help accounts

Adding a Web Remote Help Account

To add a web Remote Help account:

1. In SmartEndpoint, go to Manage > Web Remote Help Accounts.
   The Web Remote Help Accounts window opens.
2. Click New.
   The Web Remote Help Account wizard opens.
3. Select a User type:
   - Existing User/Group - AD user or group
   - Local User - Check Point user
4. Click Next.
5. Configure login credentials:

<table>
<thead>
<tr>
<th>User type &amp; Authentication</th>
<th>Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing user with AD authentication</td>
<td>a. In the Login field, type the name of a user from the AD (auto-complete field).</td>
</tr>
<tr>
<td></td>
<td>b. In the Login Method, select AD Authentication.</td>
</tr>
<tr>
<td>Existing user with Token authentication</td>
<td>a. In the Login field, type the name of a user from the AD (auto-complete field).</td>
</tr>
<tr>
<td></td>
<td>b. In the Login Method, select Token.</td>
</tr>
<tr>
<td></td>
<td>c. Click Select.</td>
</tr>
<tr>
<td></td>
<td>d. Select a token.</td>
</tr>
<tr>
<td></td>
<td>e. Click OK.</td>
</tr>
<tr>
<td>Local user with fixed password authentication</td>
<td>a. In the Login field, type the login name of a user.</td>
</tr>
<tr>
<td></td>
<td>b. In the Login Method, select Password.</td>
</tr>
<tr>
<td>User type &amp; Authentication</td>
<td>Credentials</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Local user** with Token authentication | a. In the **Login** field, type the login name of a user.  
b. In the **Login Method**, select **Token**.  
c. Click **Select**.  
d. Select a token.  
e. Click **OK**. |
| **AD Group/OU** with **AD Authentication** | a. In the **Login** field, type the name of a group from the AD (auto-complete field).  
b. In the **Login Method**, select **AD Authentication**.  
**Note** - Token authentication is not supported for AD Group/OU. |

6. Click **Next**.

7. Set the expiration date (optional):
   a) Select **Expiration**.
   b) Select a **Start Date**.
   c) Select an **Expiration Date**.

8. Set the location, if necessary:
   a) In the **Account Details** section, click **Add**.
   b) Enter a location or select one from the list.

9. Click **Finish**.

**To disable the Web Remote Help account:**

Select **Disable remote help account**. When you create a new account, it is enabled by default.

**Editing a Web Remote Help Account**

To edit a web Remote Help account:

1. In SmartEndpoint, go to Manage > Web Remote Help Accounts.  
   The **Web Remote Help Accounts** window opens.

2. Select an existing account from the list.

3. Click **Edit**.
   The **Web Remote Help Account Configuration** window opens.

4. Change the configuration as necessary.
   **Note** - you cannot change the type of an existing account.
Deleting a Web Remote Help Account

To delete a web Remote Help account:
1. In SmartEndpoint, go to **Manage > Web Remote Help Accounts**.
   The **Web Remote Help Accounts** window opens.
2. Select an existing account from the list.
3. Click **Delete**.
4. Click **OK**.

Searching for an Existing Web Remote Help Account

To search for an existing web Remote Help account:
1. In SmartEndpoint, go to **Manage > Web Remote Help Accounts**.
   The **Web Remote Help Accounts** window opens.
2. In the search box, type in the name of an account.
   List of results shows.

Configuring SSL Support for AD Authentication

To use Remote Help with AD password, it is necessary for the Remote Help server to connect to the domain controller with SSL.

To configure SSL Support:
1. Get an SSL certificate from your Domain Controller.
3. Run this CLI command on the Endpoint Security Management Server to activate the SSL connection:
   `$UEPMDIR/system/install/wrhAuthConfig`

Note - Web Remote Help works with LDAPS or LDAP authentication only. Mixed mode is not supported.

Web Remote Help

Administrators can use the built in Remote Help or online portal on the Endpoint Security Management Server, or create a dedicated server for the online web portal.

A dedicated server for the online web portal is supported with E80.60 and higher management. It is supported on Gaia servers only.

If there is one or more external Remote Help Server in an environment, you must use online synchronization.

Administrators can authenticate to the web portal with these authentication methods:
- Check Point Password login (default)- Configure this in SmartEndpoint
- Active Directory Password - See Configuring SSL Support for AD Authentication
- Dynamic Token
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:

2. Select the type of assistance the end-user needs:
   a) One Time Login - Gives access as an assumed identity for one session without resetting the password.
   b) Remote password change - This option is for users who have forgotten their fixed passwords.
3. In the User Name field, click Browse and select the user in the Select a Node window.
4. Select the locked computer in the Device Name list.
5. Click Generate Response.
6. Tell the user to enter the Response One (to user) text string in the Remote Help window on the locked computer.
   The endpoint computer shows a challenge code.
7. In the Challenge (from user) field, enter the challenge code that the user gives you.
8. Click Generate Response.
   Remote Help authenticates the challenge code and generates a response code.
9. Tell the user to enter the Response Two (to user) text string in the Remote Help window on the locked computer.
10. Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.

To give Full Disk Encryption Remote Help assistance from the web portal:

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:**

1. Go to **https://<Endpoint Security Management Server IP>/webrh**.
2. Enter your **User Name** and **Password** to log in to the portal. Administrators must have permission to give Remote Help.
3. Select **ME**.
4. In the **User Name** field, enter the name of the user.
5. In the **Challenge** field, enter the challenge code that the user gives you. Users get the **Challenge** from the Endpoint Security client.
6. Click **Generate Response**.
   Media Encryption & Port Protection authenticates the challenge code and generates a response code.
7. Give the response code to the user.
8. Make sure that the user can access the storage device successfully.
Disabling Remote Help

To disable Remote Help:

1. In the Media Encryption & Port Protection Policy window, in the Encrypt Removable Media area, click Advanced Settings.
   The Media Encryption page opens.
2. In the Offline Mode Settings expand the Advanced Settings area.
3. Clear the Allow users to recover their password using remote help option.

User-Bound Remote Help

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

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

To create a new Pre-boot user for User-bound Remote Help:

1. Use the procedure in Creating Pre-boot Users (on page 132).
2. In the Account Details window, select Do not use device information for Full Disk Encryption Remote Help.
Offline Mode

In This Section:

- Creating Offline Administrators ................................................................................. 245
- Configuring an Offline Group ........................................................................................ 246
- Configuring Policy for an Offline Group ......................................................................... 247
- Editing Pre-boot Users .................................................................................................. 248
- Exporting Packages ....................................................................................................... 249
- Deploying Packages ....................................................................................................... 251
- Moving from Offline to Online Mode .............................................................................. 251
- Endpoint Offline Management Tool .............................................................................. 252

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

- Full Disk Encryption
- OneCheck User Settings
- Client Settings

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

Workflow to Configure Offline Mode:

1. In the Users and Computers tab, create a new Offline Group and configure the sub-paths and settings (on page 246).
2. From the Offline Group, configure the policy for each blade (on page 247).
3. Export the required packages and put them in the configured sub-paths (on page 249).
4. Instruct users to install the packages from the sub-paths. Make sure they have the required access (on page 251).

Creating Offline Administrators

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

To create offline administrators:

1. Open SmartEndpoint Manager.
2. On the Users and Computers tab, right-click an offline group.
3. Select **Create Administrators**.
   The **Create offline group administrators** window opens with these options:
   - **Add Single User** - Adds one administrator
     - Enter the **Logon Name**.
     - Configure **Authentication credentials**, password or dynamic token.
     **Note** - you must select an existing token.
   - **Add Users From File** - Imports offline administrators from a CVS file, and shows them in the table.
     Each imported administrator has a Logon Name, Authentication type and status.
     The **Status** column shows if an Administrator can be imported or not.
     A green V indicates if the offline administrator is ready for import.
     An X icon indicates offline administrators that cannot be imported. See the error message next to it.
   - **Remove User** - Removes an offline administrator. Select the administrator in the table.

4. Click **Import** to import the administrators.
5. Click **OK**.

### Configuring an Offline Group

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

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

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

To create an Offline Group:

1. In the **Users and Computers** tab navigation tree, right-click on **Offline Groups** and select **New Offline Group**.
   The **New Offline Group** wizard opens
2. Enter this information:
   - **Offline group name** - A name for the group
   - **Root Path** - The root path of the shared location where files for this group are stored. This must be a valid UNC path or HTTP/HTTPS path. For example `\server\share\` or `http://server/share/`. HTTP/HTTPS paths are only supported when the WebDAV extension is enabled on the web server.
   - **Description** (optional) - Helpful information about the group or policies
3. Click **Sub-paths**.
The Sub-path Settings window opens.

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

5. Click **OK**.

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

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

### Configuring Policy for an Offline Group

**Authorize Pre-boot Users**

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

- Click **Add** to add an authorized user
- Click **Remove** to remove a user
  
  **Note** - Removing a user from the Authorized Pre-boot user list will not remove the user from an already installed client. Use the **Blocked Users** feature to remove users on clients.

- Click **Show all users** to show the complete list
- Enter text in the **Search** field to search the list of users
- Click **Blocked Users** to create a list of users who are blocked from all computers in the offline group

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

**Full Disk Encryption Policy**

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


**OneCheck User Settings Policy**

- Continue with the **New Offline Group** wizard or click **OneCheck User Settings** to configure the OneCheck User Settings policy settings for the group.

  This policy will be the default **OneCheck User Settings** policy for acquired users and users created from the deployment users on the computer. The default policy can be updated with a policy Update.

  If users are defined in SmartConsole, you can assign a different **OneCheck User Settings** policy to them in SmartEndpoint. If users are acquired and not defined in SmartConsole, they always get the default policy.

Client Settings Policy

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


Completing the Wizard

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

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

  Note - From the Group Details view, click Pre-boot Users to open:
  • The Authorized Pre-boot Users list
  • The Blocked Pre-boot Users list.

Editing Pre-boot Users

To edit offline Pre-boot accounts:

1. From the Users and Computers tab, expand an Offline Group to see the users.
2. Right-click the user and select User Authentication (OneCheck) > Pre-boot Authentication method.
3. Select an Authentication Method.
4. Click Change Password or User Certificates to create a new password or upload certificates, as required for the authentication method.
5. Click OK.

To edit a deployment Pre-boot account:

1. From the Users and Computers tab, open Offline Groups.
2. Select the preboot user account
3. Select Deployment Pre-boot User Details and click Edit.

To create offline Pre-boot users

1. From the Users and Computers tab, select an offline group.
2. In Group Details, click Edit.
  The Group Details window opens.
3. Click Pre-boot Users.
  The Pre-boot Users Details window opens.
4. In the Authorized Preboot Users area, click New.
  The Add new preboot user window opens.
5. Enter a Logon Name

6. In the Authentication credentials area, select Password or Dynamic Token.
   - A password must contain at least five characters
   - If you select a token as the authentication method, make sure you select an existing token

7. To set more granular account controls, open Account Details.

In Account Details you can configure the type of use and expirations settings.

- **Regular User** (default)
  - **Do not use device information for Full Disk Encryption remote help** - Enables user-bound remote help for the pre-boot user
  - **Lock user for preboot** - Locks the user for preboot
  - **Require change password after first logon** - Applies only to password authentication. Select this option to force users to change their password after the first pre-boot logon.

- **Deployment User**
  - **Allow creating X Pre-boot accounts from this account** - You can use this account to create new offline Pre-boot accounts. After it creates the maximum numbers of accounts allowed, the account expires.

- **Expiration Settings**:
  - The user will expire after X logins to Pre-boot
  - The user will be revoked after the selected date.

### Exporting Packages

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

**To export packages:**

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Update Policy File</td>
<td>Exports a file with policy updates.</td>
<td>This file has CPPOL extension. You must put the CPPOL file in the Updates folder.</td>
</tr>
<tr>
<td>Get Offline Management File</td>
<td>Exports a CPOMF file that contains definitions that you can use to log in to the Endpoint Offline Management Tool.</td>
<td>This is for a help desk or contractor environment that needs access to the Tool for Remote Help and creation of recovery media without access to an Endpoint Security server.</td>
</tr>
<tr>
<td>Full Disk Encryption &gt; Get Bypass Pre-boot File</td>
<td>When installed, the computer bypasses Pre-boot based on the policy configured in the Pre-boot Protection &gt; Temporary Pre-boot Bypass settings of the Offline group.</td>
<td>You must put the CPPOL file in the Updates folder.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Full Disk Encryption &gt; Get Revert Pre-boot to Policy Configuration File</strong></td>
<td>Returns the computer to the regular Pre-boot policy.</td>
<td>You must put the CPPOL file in the Updates folder.</td>
</tr>
<tr>
<td><strong>Deployment &gt; Get Initial Package</strong></td>
<td>Exports a complete MSI with the Offline Policy. This can be used for new client installation.</td>
<td></td>
</tr>
<tr>
<td><strong>Deployment &gt; Get Upgrade Package</strong></td>
<td>Exports a package to upgrade an existing offline client, and the updated CPPOL file. The details of the package are shown. Make sure the version is higher than the currently installed client version. You can select the <strong>Export update offline policy</strong> option to export a CPPOL file with the package.</td>
<td>Put the CPPOL file in the configured Updates folder and put the MSI in the configured Upgrades folder.</td>
</tr>
<tr>
<td><strong>Deployment &gt; Get Offline to Online File</strong></td>
<td>Exports a file that converts an offline client to an online client. After installation, the client will connect to the server that the file was exported from.</td>
<td>You must put the CPPOL file in the Updates folder. See Moving from Offline to Online Mode (on page 251) for best practices.</td>
</tr>
</tbody>
</table>

To export all offline administrators:

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

To replace the installation policy file for the offline group:

This is only necessary if you installed a client with an installation policy that contains shares that the client cannot access. The client remains in the installation state as the recovery file cannot be uploaded to the share.

1. In the **Users and Computers** tab, right-click on the Offline Group and select **Advanced > Get Install Policy File**.
2. Replace the installation policy located in the local Work folder on the client. The Work folder with the policy is located in:
   - On x64 client:
     - %PROGRAMFILES(X86)%%\CheckPoint\Endpoint Security\Endpoint Common\Work\%
   - On x86 client:
     - %PROGRAMFILES%\CheckPoint\Endpoint Security\Endpoint Common\Work\%
3. Reboot to continue the installation.
Deploying Packages

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

To push a policy update for a specified client:
Place the policy in the Work folder locally on the client, for example:
C:\Program Files\CheckPoint\Endpoint Security\Endpoint Common\Work.
If the client finds an update policy in the Work folder, the client makes sure that the update is new, imports it, and deletes the update from the Work folder.
The client then continues to use the normal update interval as configured.

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

Client Connections to Network Shares
Clients use the currently logged-in user to connect to the defined shares and search for update policies and to upload recovery files, logs, and status files. If there is no user logged-in or if multiple users are logged-in, the connection to the share is not available.
The logged-in user on the client must have these permissions on the share to be able to update and download files:

<table>
<thead>
<tr>
<th>Location</th>
<th>Required Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read</td>
</tr>
<tr>
<td>Update Directory</td>
<td>✔️</td>
</tr>
<tr>
<td>Recovery Files Directory</td>
<td>✔️</td>
</tr>
<tr>
<td>Client Log Directory</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Moving from Offline to Online Mode

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

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

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

---

**Endpoint Offline Management Tool**

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

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


**Logging In to the Offline Tool**

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

1. Open the Offline Tool.
2. In the Login window:
   - **CPOMF File** - Browse to the location of the CPOMF file
   - **Login Name** - Enter an offline administrator name
   - **Password/Token** - According to the authentication method of the offline administrator, enter a password or token response.

     **Note** - If the authentication method is a token with a response length of 16 digits and you are authenticating with a response that is 8 digits long, you will be prompted to complete an additional challenge-response phase.

   - Click **Login**.

**Password Assistance**

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

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

- **Select Recovery File** - The recovery file is a CPREC file that is uploaded from each client computer. The files are located in the Recovery Files shared folder.

  Click **Browse** to locate the file for the computer in the offline group that requires recovery.

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

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

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

Response to User
- **Response Two** - Tell the user to enter the Response Two text string in the Remote Help window on the locked computer.
  Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.
- **Try Again** - Click this to start the password recovery process again for a different user.

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

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

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

- Select the type of recovery media to generate:
  - ISO file
  - REC file
  - USB media
  If you select ISO or REC, select the storage location.
  If you select USB, choose the drive to use.
- Click Create Media.

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