Important Information

Latest Software

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

Latest Documentation

The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=12286

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 October 2011</td>
<td>Added a detail about uninstalling the Edge Compatibility package to Installing a Server for High Availability (on page 21).</td>
</tr>
<tr>
<td>06 September 2011</td>
<td>Updated Troubleshooting Authentication (“Troubleshooting Authentication in Server Logs” on page 47).</td>
</tr>
<tr>
<td>15 June 2011</td>
<td>First release of this document.</td>
</tr>
</tbody>
</table>

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security Management Server E80.20 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Overview of the System Architecture</td>
<td>10</td>
</tr>
<tr>
<td>Optional System Components</td>
<td>11</td>
</tr>
<tr>
<td>Software Blades</td>
<td>11</td>
</tr>
<tr>
<td>Endpoint Security Services and Ports</td>
<td>12</td>
</tr>
<tr>
<td>Centralized Organization of Users and Computers</td>
<td>13</td>
</tr>
<tr>
<td>Organization-Centric model</td>
<td>13</td>
</tr>
<tr>
<td>Policy-centric Model</td>
<td>13</td>
</tr>
<tr>
<td>Centralized Deployment</td>
<td>13</td>
</tr>
<tr>
<td>Centralized Monitoring</td>
<td>13</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>13</td>
</tr>
<tr>
<td>Installing Endpoint Security Servers</td>
<td>14</td>
</tr>
<tr>
<td>Planning Endpoint Security Management Server Installation</td>
<td>14</td>
</tr>
<tr>
<td>Prerequisites for Installation</td>
<td>15</td>
</tr>
<tr>
<td>Installing the Endpoint Security Management Server</td>
<td>16</td>
</tr>
<tr>
<td>Management Server Configuration in the Configuration Tool</td>
<td>17</td>
</tr>
<tr>
<td>Management Server Configuration in the Console</td>
<td>17</td>
</tr>
<tr>
<td>Users Created at Installation</td>
<td>18</td>
</tr>
<tr>
<td>Configuring the Apache Cache</td>
<td>18</td>
</tr>
<tr>
<td>Viewing Scheduled Tasks</td>
<td>18</td>
</tr>
<tr>
<td>Changing the Clean Up Task Status</td>
<td>18</td>
</tr>
<tr>
<td>Scheduling a New Clean up</td>
<td>19</td>
</tr>
<tr>
<td>Installing Endpoint Security Management Console</td>
<td>19</td>
</tr>
<tr>
<td>Installing External Endpoint Policy Servers</td>
<td>19</td>
</tr>
<tr>
<td>Policy Server Configuration in the Configuration Tool</td>
<td>19</td>
</tr>
<tr>
<td>Policy Server Configuration in the Console</td>
<td>20</td>
</tr>
<tr>
<td>Installing a Server for High Availability</td>
<td>21</td>
</tr>
<tr>
<td>Secondary Server Configuration in the Configuration Tool</td>
<td>21</td>
</tr>
<tr>
<td>Secondary Server Configuration in the Console</td>
<td>21</td>
</tr>
<tr>
<td>Upgrading an Endpoint Security Management Server</td>
<td>22</td>
</tr>
<tr>
<td>Troubleshooting SIC Trust</td>
<td>23</td>
</tr>
<tr>
<td>Active Directory Scanner</td>
<td>23</td>
</tr>
<tr>
<td>Configuring the Directory Scanner for the First Time</td>
<td>24</td>
</tr>
<tr>
<td>Configuring a Directory Scanner Instance</td>
<td>24</td>
</tr>
<tr>
<td>Enabling or Disabling a Scanner Instance</td>
<td>26</td>
</tr>
<tr>
<td>Directory Synchronization</td>
<td>26</td>
</tr>
<tr>
<td>Troubleshooting the Directory Scanner Configuration</td>
<td>26</td>
</tr>
<tr>
<td>Role-Based Administration</td>
<td>27</td>
</tr>
<tr>
<td>Endpoint Security Administrator Roles</td>
<td>27</td>
</tr>
<tr>
<td>Endpoint Security Licenses</td>
<td>31</td>
</tr>
<tr>
<td>Endpoint Security License Types</td>
<td>31</td>
</tr>
<tr>
<td>Demo and Product Licenses</td>
<td>31</td>
</tr>
<tr>
<td>License Behavior</td>
<td>32</td>
</tr>
<tr>
<td>Getting Licenses</td>
<td>32</td>
</tr>
<tr>
<td>Getting and Applying Contracts</td>
<td>32</td>
</tr>
<tr>
<td>License Status</td>
<td>33</td>
</tr>
<tr>
<td>Deploying Endpoint Security Clients</td>
<td>34</td>
</tr>
<tr>
<td>Deployment Overview</td>
<td>34</td>
</tr>
<tr>
<td>The Initial Client</td>
<td>34</td>
</tr>
<tr>
<td>Getting the Initial Client from the Console</td>
<td>35</td>
</tr>
<tr>
<td>Distributing the Initial Client</td>
<td>35</td>
</tr>
</tbody>
</table>
Managing Policies and Users

Managing Networks

Online Upgrades

Upgrading with Assignment

Configuring Authentication Settings

Configuring Active Directory for Authentication

Endpoint Security Active Directory Authentication

Inherited Assignment

Enforcing Policies According to States

State of Compliance

Anti-Malware

Full Disk Encryption

WebCheck

Software Packages

Seeing the Deployment Status

Using the Endpoint Security Management Console

Distributing Software Blade Packages and Updates

Distributing with Assignments

Distributing by Exporting the Package

Installing the Client Using the CLI

Troubleshooting the Installation

Client logging

Uninstalling the Client

Evaluation Mode Client

Assigning Policies

Configuring the Heartbeat Interval

Managing Policies and Users

About Policies

State of Compliance

Non-Compliance

Enforcing Policies According to States

User Policy or Computer Policy

Configuring the Heartbeat Interval

Assigning Policies

Direct Assignment

Inherited Assignment

Policy Assignment Order

Group Assignment Priority

Recommendations for Management

Viewing Assignments

Deploying Policies

Managing Users
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing a User's Password</td>
<td>67</td>
</tr>
<tr>
<td>Managing OUs or Groups</td>
<td>67</td>
</tr>
<tr>
<td>Disabling the Preboot Temporarily</td>
<td>67</td>
</tr>
<tr>
<td>Managing Computers</td>
<td>68</td>
</tr>
<tr>
<td>Managing Users of a Computer</td>
<td>68</td>
</tr>
<tr>
<td>Resetting a Computer</td>
<td>69</td>
</tr>
<tr>
<td><strong>Management High Availability</strong></td>
<td>70</td>
</tr>
<tr>
<td>Overview of High Availability in Endpoint Security</td>
<td>70</td>
</tr>
<tr>
<td>The High Availability Environment</td>
<td>70</td>
</tr>
<tr>
<td>High Availability Deployment Considerations</td>
<td>70</td>
</tr>
<tr>
<td>Active versus Standby</td>
<td>71</td>
</tr>
<tr>
<td>Changing a Server to Active or Standby</td>
<td>71</td>
</tr>
<tr>
<td>Synchronizing the Active and Standby Endpoint Security Management Servers</td>
<td>72</td>
</tr>
<tr>
<td>What Data is Synchronized?</td>
<td>73</td>
</tr>
<tr>
<td>Synchronization Status</td>
<td>73</td>
</tr>
<tr>
<td>When Synchronization Fails</td>
<td>73</td>
</tr>
<tr>
<td>Understanding the Status of the High Availability Environment</td>
<td>74</td>
</tr>
<tr>
<td>Updating the PAT Version on the Server</td>
<td>74</td>
</tr>
<tr>
<td><strong>External Endpoint Policy Servers</strong></td>
<td>76</td>
</tr>
<tr>
<td>Overview of Endpoint Policy Servers</td>
<td>76</td>
</tr>
<tr>
<td>How do Endpoint Policy Servers Work?</td>
<td>76</td>
</tr>
<tr>
<td>Configuring Policy Server Settings</td>
<td>77</td>
</tr>
<tr>
<td>Endpoint Policy Server Proximity Analysis</td>
<td>77</td>
</tr>
<tr>
<td>Enabling the Management Server to be a Policy Server</td>
<td>77</td>
</tr>
<tr>
<td>Policy Server and Management Server Communication</td>
<td>78</td>
</tr>
<tr>
<td>Configuring Log Forwarding</td>
<td>78</td>
</tr>
<tr>
<td>Monitoring Endpoint Policy Server Activity</td>
<td>79</td>
</tr>
<tr>
<td><strong>Backup and Restore</strong></td>
<td>80</td>
</tr>
<tr>
<td>Overview of Backup and Restore</td>
<td>80</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>80</td>
</tr>
<tr>
<td>How to Back Up and Restore</td>
<td>80</td>
</tr>
<tr>
<td>Updating the PAT Version on the Server after Restore</td>
<td>81</td>
</tr>
<tr>
<td><strong>OneCheck User Settings Policies</strong></td>
<td>82</td>
</tr>
<tr>
<td>Quick Start</td>
<td>82</td>
</tr>
<tr>
<td>Seeing OneCheck User Settings Policy Assignments</td>
<td>83</td>
</tr>
<tr>
<td>OneCheck User Settings Assignments</td>
<td>83</td>
</tr>
<tr>
<td>Configuring OneCheck User Settings</td>
<td>83</td>
</tr>
<tr>
<td>Account Lockout</td>
<td>83</td>
</tr>
<tr>
<td>Password Security</td>
<td>84</td>
</tr>
<tr>
<td>OneCheck User Settings Permissions</td>
<td>85</td>
</tr>
<tr>
<td><strong>Full Disk Encryption Policies</strong></td>
<td>87</td>
</tr>
<tr>
<td>Overview of Full Disk Encryption</td>
<td>87</td>
</tr>
<tr>
<td>Quick Start</td>
<td>87</td>
</tr>
<tr>
<td>Seeing Full Disk Encryption Policy Assignments</td>
<td>88</td>
</tr>
<tr>
<td>Creating a Customized Full Disk Encryption Policy</td>
<td>88</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>88</td>
</tr>
<tr>
<td>Preboot Protection</td>
<td>89</td>
</tr>
<tr>
<td>User Acquisition</td>
<td>93</td>
</tr>
<tr>
<td>OneCheck Logon</td>
<td>94</td>
</tr>
<tr>
<td>Policy Assignment</td>
<td>94</td>
</tr>
<tr>
<td>Full Disk Encryption Installation and Deployment</td>
<td>95</td>
</tr>
<tr>
<td>Client Requirements for Full Disk Encryption Deployment</td>
<td>95</td>
</tr>
<tr>
<td>Completing Full Disk Encryption Deployment on a Client</td>
<td>96</td>
</tr>
<tr>
<td>Stages of the Deployment Phase</td>
<td>96</td>
</tr>
<tr>
<td>Primary Full Disk Encryption Components</td>
<td>96</td>
</tr>
<tr>
<td>Full Disk Encryption Recovery</td>
<td>97</td>
</tr>
<tr>
<td>Creating Data Recovery Media</td>
<td>97</td>
</tr>
<tr>
<td>Using Data Recovery Media</td>
<td>98</td>
</tr>
<tr>
<td>Upgrading Full Disk Encryption</td>
<td>98</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction


Check Point Endpoint Security is an Organization-Centric based management, providing security and unique visibility for users in the organization, not just computers.

Features:

- Single management and console for endpoint security management
- Monitor your security status with a customizable, at-a-glance dashboard
- Quickly deploy the required protection for users via software-blade deployment profiles
- Manage endpoint security from the entire organization to groups, users and their devices
- Use Pre-configured and customizable policies
- Easily modify, track and report security policy changes at all levels of the organization
- Drill-down on users and all their associated machines to investigate security status
- Enforce and remediate endpoints’ compliance before accessing corporate network

In This Chapter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of the System Architecture</td>
<td>10</td>
</tr>
<tr>
<td>Software Blades</td>
<td>11</td>
</tr>
<tr>
<td>Endpoint Security Services and Ports</td>
<td>12</td>
</tr>
<tr>
<td>Centralized Organization of Users and Computers</td>
<td>13</td>
</tr>
<tr>
<td>Centralized Deployment</td>
<td>13</td>
</tr>
<tr>
<td>Centralized Monitoring</td>
<td>13</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>13</td>
</tr>
</tbody>
</table>
Overview of the System Architecture

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

### Endpoint Security Management Server

<table>
<thead>
<tr>
<th>Number</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Endpoint Security Management Console</strong> - Application installed on a Windows platform that lets you deploy, monitor, and configure Endpoint Security clients and policies. You can install an <strong>Endpoint Security Management Console</strong> on the <strong>Endpoint Security Management Server</strong> or on a computer that supports the client installation.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Endpoint Security Management Server</strong> - Computer that contains the Endpoint Security software and databases. The <strong>Endpoint Security Management Server</strong> communicates with endpoint clients to manage client policies and to update protections.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Endpoint Security Blades</strong> - Library of software blades available on the Endpoint Security Management Server. You can install any or all of these blades on individual endpoint clients.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Endpoint Security Database</strong> - Contains the policy that enforces security on endpoint clients. This database also contains user and computer objects, licensing and Endpoint monitoring data.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Directory Scanner Configuration</strong> - Software component that synchronizes the structure and contents of the <strong>Active Directory</strong> with the Endpoint Security policy database.</td>
</tr>
</tbody>
</table>

### Endpoint Security Clients

<table>
<thead>
<tr>
<th>Number</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><strong>Endpoint Security clients</strong> - Client application installed on end-user computers. These clients monitor the security aspects of your endpoints and enforce security policies.</td>
</tr>
</tbody>
</table>
Number | Component
--- | ---
7 | **Endpoint Agent** - Endpoint Security software component deployed on endpoint client computers. It operates as a container for 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)
8 | **Endpoint Security Blades** - Software blades deployed on the endpoint client.

**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.

**Software Blades**

The Endpoint Security Management Server includes these modular, centrally managed software blades. Each blade has one or more policies that can be configured. You can enable and configure these blades at any time to meet changing security needs.

<table>
<thead>
<tr>
<th>Blade</th>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
</table>
| Full Disk Encryption | OneCheck User Settings | Manages:  
- How a Full Disk Encryption user logs in to the computer  
- How failed logins are handled  
- Password security  
- Access to remote help. |
| Full Disk Encryption | Full Disk Encryption | Combines Preboot protection, boot authentication, and strong encryption to make sure that only authorized users are given access to information stored on desktops and laptops. |
| Media Encryption & Port Protection | Media Encryption & Port Protection | Protects data stored on the computers by encrypting removable media devices and allowing tight control over computers’ ports (USB, Bluetooth, and so on). |
| Malware Protection | Malware Protection | Protects clients from known and unknown viruses, worms, Trojan horses, adware, and keystroke loggers. |
| Firewall | Access Zones | Defines the topology of the organizational network, separating it into Trusted and Internet domains. |
| Firewall | Firewall Rules | Blocks or allows network traffic based on attributes of network connections. |
| Firewall | Application Control | Controls network access on a per-application basis, letting you restrict application access by zone and direction. |
| Firewall | Endpoint Compliance | 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. |
VPN

Remote Access VPN or Legacy Remote Access VPN lets users connect remotely to a Check Point Security Gateway using IPsec and SSL VPN.

WebCheck

WebCheck

Protects endpoint computers against phishing attacks. WebCheck creates its own virtual browser with its own file system. Changes made by a non-trusted site are confined to the virtual browser file system.

---

## Endpoint Security Services and Ports

Endpoint Security operations are implemented by different services on the Endpoint Security Management Server, the Endpoint Security Management Console, 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 Endpoint Security Management Console. 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 IPS Encrypted Protocol</td>
</tr>
<tr>
<td>• New file encryption key retrieval</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Synchronization request</td>
<td>ESP Encrypted</td>
<td>TCP/80</td>
<td>Heartbeat, communicates policy, status and compliance changes.</td>
</tr>
<tr>
<td>• Heartbeat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Log upload</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Full Disk Encryption Recovery Data Upload</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Media Encryption &amp; Port Protection Key Exchange</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Full Disk Encryption User Acquisition &amp; User credentials.</td>
<td>ESP Encrypted</td>
<td>TCP/443</td>
<td></td>
</tr>
</tbody>
</table>

The Endpoint Security Management Console uses SIC to reach the Endpoint Security Management Server:

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Secure Internal Communication</td>
<td>SIC</td>
<td>TCP/18190</td>
<td></td>
</tr>
</tbody>
</table>

Before installing Endpoint Security Management Server, make sure these ports are free:

<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>
</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 granular as you need.

Policy-centric Model

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

You create and assign policies to the root node of the organizational tree as a property of each Endpoint Security blade. Policies can be deployed one by one all or all together. As different groups, networks, OUs, computers, or users develop different security needs, adjust the different blade configurations accordingly.

Centralized Deployment

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

Centralized Monitoring

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

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

Related Documentation

For information about requirements for this release, see the Endpoint Security E80.20 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11910).

Chapter 2

Installing Endpoint Security Servers

See the E80.20 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11910) for supported platforms for installation.

In This Chapter

Planning Endpoint Security Management Server Installation 14
Prerequisites for Installation 15
Installing the Endpoint Security Management Server 16
Users Created at Installation 18
Configuring the Apache Cache 18
Installing Endpoint Security Management Console 19
Installing External Endpoint Policy Servers 19
Installing a Server for High Availability 21
Upgrading an Endpoint Security Management Server 22
Troubleshooting SIC Trust 23
Active Directory Scanner 23
Role-Based Administration 27

Planning Endpoint Security Management Server Installation

Before you begin installation, check these items:

- The diagram below shows installation options, where (1) represents the Endpoint Security Management server and (2) represents the Endpoint Policy Server.
Decide whether to install Endpoint Policy Servers in a distributed architecture (option A); or to use only the Endpoint Policy Server embedded in the Security Management Server (option B). It is recommended that remote sites have at least one external Endpoint Policy Server on a dedicated computer for each remote site, and that large sites have multiple Endpoint Policy Servers to ensure good performance.

**Figure 2-1** Endpoint Security Installation Options

- Make sure there is connectivity between the Security Management Server and the Endpoint Policy Servers.
- Connectivity between multiple Endpoint Policy Servers is not necessary, but every client must be able to communicate with at least one Endpoint Policy Server.
- Make sure the computers on which the Endpoint Security components (Endpoint Security Management Server, Endpoint Security Management Console, and Endpoint Policy Servers) will be installed are on supported platforms (see the [E80.20 Release Notes](http://supportcontent.checkpoint.com/documentation_download?ID=11910)).
- Endpoint Security Management Server installation requires Microsoft .NET 3.5 SP1 Runtime Framework. If you have it installed in advance, the Endpoint Security installation will progress faster.
- Make sure that ports 80 and 443 are free to be used by the Endpoint Security Management Server installation.
- When an Endpoint Security client is connected to the Endpoint Security Management Server or Policy Server through a proxy, the client’s IP address might be obscured by the proxy’s IP address. To avoid this, configure the proxy to use the X-Forwarded-For HTTP header.

## Prerequisites for Installation

- Before installing Endpoint Security Management Server, make sure the required ports are free ("Endpoint Security Services and Ports" on page 12).
- If you plan to install a Endpoint Security server on Windows 2003 R2 SP2 with a French or Italian operating system, first install Microsoft fix KB971812.
Installing the Endpoint Security Management Server

To start the Endpoint Security server installation:
1. Log on as Administrator and insert the CD. The installation wizard automatically starts and a Congratulations message shows.
2. Click Forward.
3. Accept the terms of the End Users License Agreement.
4. Click Forward.
5. Select New installation.
6. Click Forward.
7. In the left pane of The Only Unified Security Platform page, select to install these products:
   - Security Management
   - Endpoint Security
   - SmartConsole
8. Click Forward.
9. On the Please specify the Security Management type page, select:
   - Primary Security Management - For the only Endpoint Security Management server in a regular deployment or the first in a High Availability deployment.
   - Secondary Security Management - For a second Endpoint Security Management server in a High Availability deployment. If you install more than two Endpoint Security Management servers, choose this option also.
10. Click Forward.
11. See the summary of the selected products. Click Forward.
12. The Installation Status window opens. You can see the progress of the installation.

Product Installation
1. In the Security Management installation, see the location where the Check Point R70 Security Management will be installed.
   - To confirm click Next.
   - To change the location, Browse to a new location and then click Next.
   Wait while the software installs.
2. Click OK when the installation is complete.
3. Wait for the Endpoint Security installation to load.
4. In the Endpoint Security installation, see the location where the Endpoint Security Management Server E80.20 will be installed.
   - To confirm click Next.
   - To change the location, Browse to a new location and then click Next.
   Wait while the software installs.
5. In the SmartConsole installation, see the location where the SmartConsole will be installed.
   - To confirm click Next.
   - To change the location, Browse to a new location and then click Next.
6. On the Select Clients page, leave all of the clients selected to install as part of the SmartConsole.
7. Click Next.
   Wait while the software installs.
8. Select if you want SmartConsole shortcuts on your desktop.
9. A message shows that the Check Point SmartConsole was installed successfully. Click OK.
10. A message shows that the Wizard is Complete and SmartConsole is installed on your computer. Click Finish.
Follow the setup status for SmartConsole clients.

11. Click Finish.

For first time installations, the Licenses and contracts window opens. This starts the Endpoint Security Management server configuration.

The Check Point Configuration Tool opens for the initial configuration of Endpoint Security products.

Management Server Configuration in the Configuration Tool

You can make changes to the configuration from Check Point Configuration Tool at a later date. To access it, select Start > Run > Check Point Configuration Tool, or enter cpconfig in the command line.

To configure the Endpoint Security Management server for the first time:
1. After installation, the Check Point Configuration Tool opens on the Licenses and Contracts window.
2. Click Fetch from File (if you have a license file), or leave it blank to use the Evaluation license.
3. Click Next.
4. If you did not add a license, a message opens that asks if you want to continue. Click Yes to continue.
5. You can add licenses at a later time.
6. In the Administrators window, click Add to add one or more Endpoint Security administrators. Enter a user name and password for each one.
   Note - Do not modify the default permissions.
7. Click Next.
8. In the GUI Clients window, enter a hostname or IP address of a computer from which an administrator can access the Endpoint Security Management Server and click Add. You can add multiple GUI Clients. To permit all computers to access the SmartConsole, enter any.
   The Certificate Authority window opens.
9. Click Next.
   The internal Certificate Authority initializes with the name in the text box.
10. Click OK.
   The Fingerprint window opens. The character string shown in the text box authenticates an Endpoint Security Management Console connecting to the Endpoint Security Management Server. We recommend that you click Export to File to save a copy.
11. Click Finish.
12. Click Yes to restart the server.

Management Server Configuration in the Console

You must configure the server as a Check Point network object in the Endpoint Security Management Console and install the Endpoint Security Management server database.

To configure the Endpoint Security Management server in the Endpoint Security Management Console:
1. After you do the steps in the Check Point Configuration Tool, open the Endpoint Security Management Console.
2. Open Manage > General Properties.
   The Host Properties window for the server opens.
4. In the Host Properties window:
   • Optionally, change the name of the server as it is shown in the SmartConsole.
   • Make sure that the IP address of the Endpoint Security Management Server object in SmartDashboard matches the IP address of the Windows server on which the Endpoint server is installed.
5. Click Install Database.
6. Select a database from the list, and click **Install**.

**Users Created at Installation**

During the server installation, a local user account called CPEP$USER is created. The account has:

- Special privileges to run Endpoint Security Management Server services.
- A hard-coded password.

**Configuring the Apache Cache**

By default, the size of the apache cache is set to 5GB. After installing the Endpoint Security Management Server, you might want to adjust the cache to a size more applicable to your hardware.

For cleaning and controlling the size of the cache directory, Apache supplies the executable tool: 
`htcacheclean`. Endpoint Security Management Server uses `cpd` (the Check Point daemon) to schedule `htcacheclean` to run at specified intervals. When running, `htcacheclean`:

- Checks the cache directories at regular intervals for removable content
- Controls the cache size.

Using the `cpd` scheduler configuration tool you can:

- View Scheduled tasks
- Change the task status
- Schedule new tasks

**Viewing Scheduled Tasks**

The default disk clean up task scheduled during installation of the Endpoint Security Management Server is called **ApacheCacheClean**. To see the task and its parameters, run:

```
# cpd_sched_config print
```

The same data is available in the Window's registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\CPShared\<version_number>\reserved\CPD_Schedul er\ApacheCacheClean

**Changing the Clean Up Task Status**

1. To stop the cache clean up, run:

   ```
   # cpd_sched_config deactivate ApacheCacheClean -r
   ```

2. To start the cache clean up, run:

   ```
   # cpd_sched_config activate ApacheCacheClean -r
   ```

   **Note** - The `deactivate` and `activate` commands refer to the scheduler's timer. Deactivate suspends the timer. Activate restarts the timer. Restarting the timer does not immediately invoke `htcacheclean`. The scheduler runs `htcacheclean` only after the specified time interval.

3. To delete the clean up task, run:

   ```
   # cpd_sched_config delete ApacheCacheClean -r
   ```

   **Note** - The `-r` flag applies the update immediately.
Scheduling a New Clean up

To schedule a new clean up task, use the \texttt{add} flag.

For example, if disk cache clean up must occur each hour (3600 seconds) and the cache directory size stay below 100MB, run:

\begin{verbatim}
# cpd_sched_config add NewApacheCacheClean -c "\"C:\Program Files\CheckPoint\CPuem\E80.20\apache22\bin\htcacheclean.exe\" -v \"-nt \-p\"C:\Program Files\CheckPoint\CPuem\E80.20\apache22\cache\" -1100M" -e 3600 -r
\end{verbatim}

After one hour, the cpd scheduler runs the new task.

\textit{Note} - Make sure to wrap the paths with double quotes exactly as shown in the example.

Installing Endpoint Security Management Console

The Endpoint Security Management Console usually installs as part of the Endpoint Security Management server installation. If it is necessary to install the GUI separately, use this procedure:

\textbf{To install directly from the CD}

1. Run the setup program directly from the installation CD: 
   
   \texttt{My_CD_Drive:Windows\CPclnt\setup.exe}.
2. The Welcome message shows.
3. Click \textbf{Next}.
4. Accept the Software license agreement.
5. Choose the destination folder for the installation.
6. When prompted to select clients for SmartConsole, leave all the options selected. Follow the setup status for SmartConsole clients.
7. Click \textbf{Yes} to create shortcuts on the desktop.
   
   A confirmation message shows.
8. Click \textbf{OK} and \textbf{Finish}.

Installing External Endpoint Policy Servers

We recommend that you use a distributed deployment of external Endpoint Policy Servers on dedicated machines. This includes:

- At least one Endpoint Policy Server for each remote site.
- In larger sites, multiple Endpoint Policy Servers to improve performance.

\textbf{To install an Endpoint Policy Server}:

1. Install an Endpoint Security Management Server according to the server installation procedures ("Installing the Endpoint Security Management Server" on page 16).
2. On the Please specify the Security Management type page, select \textbf{Endpoint Policy Server}.
3. The components that install are:
   - A Check Point R70 Log Server
   - Endpoint Security Policy Server

Policy Server Configuration in the Configuration Tool

You can make changes to the configuration from \textbf{Check Point Configuration Tool} at a later date. To access it, select \textbf{Start} > \textbf{Run} > \textbf{Check Point Configuration Tool}, or enter \texttt{cpconfig} in the command line.
To configure the Endpoint Policy Server for the first time:
1. After installation, the Check Point Configuration Tool opens on the Licenses and Contracts window.
2. Click Fetch from File (if you have a license file), or leave it blank to use the Evaluation license.
3. Click Next.
4. If you did not add a license, a message opens that asks if you want to continue. Click Yes to continue. You can add licenses at a later time.
5. In the Administrators window, add a user name and password for Endpoint Security administrators.
   
   Note - Do not modify the default permissions.
6. Click OK.
7. Click Next.
8. In the GUI Clients window, enter a hostname or IP address of a computer from which an administrator can access the Endpoint Security Management Server and click Add. You can add multiple GUI Clients. To permit all computers to access the SmartConsole, enter any.
9. Click Next.
10. In the Secure Internal Communication window, enter and confirm an Activation Key. The Activation Key is like a password. You will enter it again later in the Endpoint Security Management Console to create secure communication with the Endpoint Security Management server.
11. Click Finish.
12. Click Finish.
13. Click Yes to restart the server.

Policy Server Configuration in the Console

In the Endpoint Security Management Console, you add the Endpoint Policy Server to the list of servers and create secure communication between the Endpoint Policy Server and the Endpoint Security Management server. This also creates an object for the Endpoint Policy Server in SmartDashboard.

To create the Endpoint Policy Server in the Endpoint Security Management Console:
1. After you do the steps in the Check Point Configuration Tool, open the Endpoint Security Management Console.
2. Select Manage > General Properties.
3. Select Endpoint Policy Servers, if it is not already selected.
4. Click New.
5. In the Select New Object Type window, select Host and click OK.
   
   The Host Properties window for the server opens.
6. Enter a Name for the Endpoint Policy Server and its IP address.
7. Click Communication to create SIC communication with the Endpoint Security Management server.
8. In the Communication window:
   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 Endpoint Policy Server and the Endpoint Security Management server.
   c) If the trust is not created, click Test SIC Status to see what you must do to create the trust successfully.
   d) If you have to reset the SIC, click Reset, reset the SIC on the Policy Server ("Troubleshooting SIC Trust" on page 23) and then click Initialize.
   e) Click Close.
9. Click OK.
10. You might get an Enforce Changes message that prompts you to save the changes. Click Save & Install.
11. If you did not click Save & Install in the message, select File > Install Policies.

After the policy is installed, the Endpoint Policy Server synchronizes with the Endpoint Security Management server. This can take a long time, based on the amount of policies and installation packages that it must download from the Endpoint Security Management server.
To complete the Endpoint Policy Server configuration in the Endpoint Security Management Console:

1. Open the Endpoint Policy Server object that you created in the steps above.
2. In the object properties window, click **Install Database**. This enables the Endpoint Policy Server to collect logs.
3. After the installation process completes click **Close** in the Install Database window.
4. Click **OK**.
5. Click **OK**.
6. Click **Save**.
7. You might get an **Enforce Changes** message that prompts you to save the changes. Click **Save & Install**.
8. If you did not click **Save & Install** in the message, select **File > Install Policies**.

### Installing a Server for High Availability

You can install one or more additional Endpoint Security Management servers for High Availability. Servers used for High Availability must have the same Operating System version and the same system architecture (either 32-bit or 64-bit).

If you have a primary Endpoint Security Management server that was originally installed with R80, R80.10, or E80.20 EA, before you install a secondary server, you must do this: Uninstall the Edge Compatibility package from, the primary Endpoint Security Management server.

To install more Endpoint Security Management servers for High Availability:

1. Install an Endpoint Security Management server according to the server installation procedures ("Installing the Endpoint Security Management Server" on page 16).
2. On the **Please specify the Security Management type** page, select **Secondary Security Management**.

### Secondary Server Configuration in the Configuration Tool

To configure the secondary server for the first time:

1. After installation, the **Check Point Configuration Tool** opens on the **Licenses and Contracts** window.
2. Click **Fetch from File** (if you have a license file), or leave it blank to use the Evaluation license.
3. Click **Next**.
4. If you did not add a license, a message opens that asks if you want to continue. Click **Yes** to continue. You can add licenses at a later time.
5. In the **Secure Internal Communication** window, enter and confirm an **Activation Key**. The Activation Key is like a password. You will enter it again later in the Endpoint Security Management Console to create secure communication with the Endpoint Security Management server.
6. Click **Finish**.
7. Click **OK**.
8. Click **Finish**.
9. Click **Yes** to restart the server.

### Secondary Server Configuration in the Console

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 the SmartDashboard from **Start > Programs > Check Point SmartConsole > SmartDashboard**.
2. In the **Network Objects** tree, right-click **Check Point** and select **Host**. The Check Point Host window opens.
3. Enter a name and IP address for the server.

4. In the **Software Blades**, section, in the **Management** tab, select **Network Policy Management** and **Endpoint Policy Management**. This automatically selects the **Secondary Server** and **Logging and Status** options also.

   ![Note](Image)
   - **Note** - For the Secondary Security Management server to act as a Log Server when the Primary Security Management server becomes unavailable, additional steps must be performed. In the Security Gateway properties window, select **Logs and Masters > Log Servers**. Add the Secondary Security Management server to the **When a Log Server is unreachable, send logs to** list.

5. 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 Endpoint Policy Server and the Endpoint Security Management server.
   
c) If the trust is not created, click **Test SIC Status** to see what you must do to create the trust successfully.
   
d) If you have to reset the SIC, click **Reset**, reset the SIC on the Policy Server ("**Troubleshooting SIC Trust**" on page 23) and then click **Initialize**.
   
e) Click **Close**.

6. Select **File > Save**.

7. If there is a gateway installed on the Security Management Server, install the Security Policy on the gateway before you start the manual synchronization.

**To do the first synchronization:**

1. Manually synchronize the Secondary Security Management server with the Primary Security Management Server: In SmartDashboard, select **Policy > Management High Availability** and select **Synchronize**.

2. Manually copy new MSI files from the Active ESM to the Standby ESM:
   
a) On the Active ESM, copy `%fwdir%\conf\SMC_Files\uepm\MSI`.
   
b) On the Standby ESM, replace the `%fwdir%\conf\SMC_Files\uepm\MSI` file with the file from the Active server.


4. Open the Endpoint Security Management Console, connected to the Primary Security Management Server, and select **File > Install Policies**.

5. Select the **General Properties** policy and click **Install**.

The servers automatically synchronize again.

If you configured manual synchronization only in the SmartDashboard, synchronize manually.

   ![Note](Image)
   - **Note** - While the synchronization takes place, the SmartDashboard shows **Not Responding**.

You can use the SmartDashboard and Endpoint Security Management Console on the secondary server in Read Only mode.

---

**Upgrading an Endpoint Security Management Server**

To upgrade Endpoint Security Server to this version:

2. Extract the TGZ file locally on the Server.
3. Run Setup.exe.
   A command prompt window opens asking if you want to continue.
4. Type: y
5. Reboot when prompted.
6. Download the E80.20 SmartConsole from the Check Point Support Center (http://supportcenter.checkpoint.com) or from the Endpoint Security Management Server E80.20 for Windows CD > Windows /CPclnt folder.
7. Click setup.exe.
8. When prompted, click Remove to uninstall the earlier SmartConsole that you have installed.
9. When it completes, click setup.exe again to install the E80.20 SmartConsole.

Troubleshooting SIC Trust

If you cannot successfully create SIC trust on a server, it might be necessary to reset SIC on a peer server.

To reset SIC on a Policy Server:

1. In the CLI of the server, run cpconfig.
   The Check Point Configuration Tool opens.
2. Select the Secure Internal Communication tab.
3. Click Reset.
4. Click Yes.
5. Enter an Activation key and confirm it.

If you cannot create a state of trust between the Endpoint Security Management server and Endpoint Policy Server and get this message:

   SIC Status for CP: Unknown
   Could not establish TCP connection with <Policy Server IP address>

- Make sure that the CPD process is running on the Endpoint Policy Server and that TCP connectivity is allowed from the Security Management Server to the IP address of the Endpoint Policy Server on port 18191.
- Make sure that the Windows Server firewall on the Endpoint Security Management server does not drop Check Point communication.

Active Directory Scanner

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

When you first login to the Endpoint Security Management Console, the My Organization tree is empty. To populate the tree with users from the active directory, you must configure the Directory Scanner Configuration.

The Directory Scanner scans the defined Active Directory and fills the Directories node in the My Organization tab, copying the existing Active Directory structure to the server database. For this to succeed, the user account associated with the Directory Scanner requires read permissions to:

- All Active Directory paths that will be scanned.
- The deleted objects container.
An object deleted from the Active Directory is not immediately erased but moved to the Deleted Objects container. Comparing objects in the AD with those in the Deleted objects container gives a clear picture of network resources (computers, servers, users, groups) that have changed since the last scan. For additional information, see the Microsoft Knowledge Base (http://support.microsoft.com/default.aspx?scid=kb;en-us;892806).

Note - When using multi-domain scanning, you must configure the service with an account that has read permissions for all required domains and for the deleted object container for each domain. For the account to access all the scanned domains, they must have a trust relationship.

Configuring the Directory Scanner for the First Time

Until you configure it, each time you open the Directory Scanner, a message shows that asks if you want to configure the Directory Scanner. When you click Configure the Directory Scanner, the messages show you how to configure the scanner for the first time and set up a scanner instance.

A scanner instance defines which path of the active directory will be scanned and how often. One scanner instance can include the entire active directory.

Note - Scanning large numbers of Active Directory objects can affect performance.

To configure the Directory Scanner for the first time:

1. Make sure the Endpoint Security Management Server is installed on a computer listed in the Active Directory
2. Make sure you have an account to the Domain Administrator group or Domain User group with Read permissions to:
   - All paths that will be scanned
   - The Deleted Objects container
     Note - We recommend that you create a specified account for this purpose and make sure that this account's password never expires.
5. If the credentials are set to Local System, the Windows Service Credentials window opens. Enter the account, and password details for the user defined in step 2. A message shows when the credentials are updated successfully.
6. Click OK.
7. A message shows:
   Do you want to add a Scanner Instance now?
   Click Yes to add a Scanner Instance.
8. Go to step 4 in Configuring a Directory Scanner Instance (on page 24).

Configuring a Directory Scanner Instance

A scanner instance defines which path of the active directory will be scanned and how often. One scanner instance can include the entire active directory.

If you created a scanner instance when you configured the directory scanner for the first time, it might not be necessary to configure a different scanner instance. A new scanner instance is only necessary to scan a different domain or path of the active directory.

To create a scanner instance:

1. Open the Endpoint Security Management Console > My Organization tab.
3. Click Add.
4. In the Domain Name window, enter the domain name in FQDN format, for example, mycompany.com.

5. Click OK.

   The **Directory Access Credentials** window opens.
   This information is used to automatically fetch the LDAP hierarchical tree. You can click **Skip** to skip this step and manually enter the LDAP path to be scanned.

6. Enter the directory access credentials.
   - Domain
   - DC Host (Domain Controller host)
   - User name (of an account with the required credentials)
   - Password
   If available, the fields are filled in automatically.

7. Click OK.
   The **Directory Scanner Configuration** window opens.

8. Fill in these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner Name</td>
<td>A name for the scanner instance.</td>
</tr>
<tr>
<td>Scan Interval</td>
<td>The interval, in minutes, between scans to maintain an updated directory.</td>
</tr>
<tr>
<td>LDAP Path</td>
<td>Enter the full LDAP path according to the format: LDAP://&lt;Domain-Controller Host Name&gt;/&lt;Root DN&gt; where:</td>
</tr>
<tr>
<td></td>
<td>- Domain-Controller Host Name: the name of the domain controller.</td>
</tr>
<tr>
<td></td>
<td>- Root DN: The search base root distinguished name. Usually, the distinguished name of the domain name.</td>
</tr>
<tr>
<td></td>
<td>The root search base can also be an OU in the domain. For example: OU=Users,OU=Europe,OU=Enterprise,DC=mycompany,DC=com or CN=Users,DC=mycompany,DC=com.</td>
</tr>
<tr>
<td></td>
<td>The directory scanner scans all objects under the selected OU.</td>
</tr>
</tbody>
</table>

   **Note** - If a defined search base contains AD groups with members that are not in this search base, the scanner will scan these members.

   To prevent scanning outside the defined OU, create an AD account with permissions for this OU and its children.

   If NetBIOS is disabled in your Active Directory environment, use the FQDN of the Domain Controller instead of the Domain Controller's computer name.

   Alternatively, select the desired OU from the graphic tree simulation. The correct LDAP path shows in the text field.

In the **Directory Scanner** window, the above data plus **status** details show in the table.

The **Scan Status** can be:
- **Waiting for First Scan** - The scanner instance has never run.
- **Pending** - Waiting for a scan to occur again.
- **Scanning** - In the process of scanning.
- **Completed** - The scan was successful.
- **Disabled** - This scanner instance will not occur.
- **Insufficient Credentials** - The Windows service credentials were not set correctly
- **Service Inactive** - The Windows service that does the scan is not running.

9. The scan occurs according to its schedule.

   **Note** - Scanning the Active Directory takes time. AD objects show in the sequence they are discovered.
Enabling or Disabling a Scanner Instance

After a scan is configured, you can disable it to prevent it from occurring, or enable it if it was disabled.

To enable or disable a scanner instance:
1. In the Endpoint Security Management Console go to Tools > Directory Scanner. The Directory Scanner window shows a list of the configured scanner instances.
2. In the Enabled column:
   - Clear the checkbox to disable a scan.
   - Select the checkbox to enable a scan.
3. Click Close.

Directory Synchronization

At the specified interval of a scanner instance, the Directory Scanner synchronizes Endpoint Security nodes in the My Organization 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 calculation.
- Deleted users are removed from the My Organization tree, but only if they had no encrypted removable media devices. Deleted users with encrypted removable media devices move to the Other Users/Computers folder. Even though the user no longer exists in the Active Directory, the server keeps the encryption keys for possible recovery.
- Computers deleted from the AD that do not have Endpoint Security are deleted from My Organization.
- Computers deleted from the AD that do have Endpoint Security move to the Other Users/Computers folder because they may 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 remain unchanged.

Troubleshooting the Directory Scanner Configuration

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The account of the Directory Scanner service 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>

Using the cpADscanner log file

Open the Directory Scanner log file: %uepmdir%/logs/cpADscanner.log

- Possible cpADscanner entry:

Possible causes:
- Connectivity problems exist between the Endpoint Security server and the Domain Controller.
Role-Based Administration

After installing the Endpoint Security Management server, you need to assign administrator roles ("Endpoint Security Administrator Roles" on page 27).

To assign an Endpoint Security administrator role:
1. On the Endpoint Security Management server open Start > All Programs> CheckPoint SmartConsole R70 > SmartDashboard.
   The SmartDashboard opens.
2. Click Manage > Users and Administrators.
   The Users and Administrators window opens.
3. Click New > Administrator.
   The Administrator Properties window opens.
4. Enter the administrator Login Name and click New to assign the permissions profile.
   The Permissions Profile Properties window opens.
5. Enter the administrator name.
6. In the Permissions area, select Customized and click Edit.
   The Permissions Profile Custom Properties window opens.
   Selecting this option adds a tab for Endpoint Security Server.
   Note - Selecting Read/Write or Read-Only permissions for this option has no influence on functionality. You can safely select either.
8. Click the Endpoint Security tab.
   Four administrator roles are available from the drop-down box:
   • Full Access ("Full Access Role" on page 28)
   • Help Desk ("Help Desk Role" on page 29)
   • Read Only ("Read Only Role" on page 30)
   • Remote Help (on page 30)
9. Select an administrator Role.
10. In addition to the Role, you can select the Remote Help and/or Install Policies options.
    • To give the administrator permission to give Remote Help, you must select Remote Help.
    • To give the administrator permission to give install Policies, you must select Install Policy.
11. Click OK.
   Note - On the Administration Properties window, click View Profile to display the administrator's profile settings.

Endpoint Security Administrator Roles

This section covers the permissions available for Endpoint Security administrator roles.
Note - By default, on the General tab the Objects database option is always selected and cannot be cleared.

**Full Access Role**

<table>
<thead>
<tr>
<th>Object database Permission on General tab</th>
<th>Options selected on Endpoint Security tab</th>
<th>The Administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Policy</td>
<td>Remote Help</td>
<td></td>
</tr>
<tr>
<td><strong>Read Only</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| <strong>Read/ Write</strong> | Yes | Yes | • Creates, modifies, or deletes Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console. |
| | | | • Installs all types of Endpoint Policy |
| | | | • Gives remote help for: |
| | | | • User Preboot logon |
| | | | • Media Encryption &amp; Port Protection |
| Yes | No | | • Creates, modifies, or deletes Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console. |
| | | | • Install all kinds of Policy |</p>
<table>
<thead>
<tr>
<th>Install Policy</th>
<th>Remote Help</th>
<th>The Administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>• Creates, modifies, or deletes Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Give remote help for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Preboot logon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Creates, modifies, or deletes Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console.</td>
</tr>
</tbody>
</table>

**Help Desk Role**

<table>
<thead>
<tr>
<th>Install Policy</th>
<th>Remote Help</th>
<th>The Administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>• Has Read access to all the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Has write access the Software Deployment policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cannot create, modify, or delete Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Installs the Software Deployment policy (only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gives remote help for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Preboot logon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>• Has Read access to all the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cannot create, modify, or delete Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Has write access the Software Deployment policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Installs the Software Deployment policy (only)</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>• Has Read access to all the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cannot create, modify, or delete Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Has write access the Software Deployment policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gives remote help for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Preboot logon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
</tbody>
</table>
## Role-Based Administration

<table>
<thead>
<tr>
<th>Object database</th>
<th>Options selected on Endpoint Security tab</th>
<th>The Administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td>Install Policy</td>
<td>Remote Help</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Read Only Role

<table>
<thead>
<tr>
<th>Object database</th>
<th>Remote Help selected on the Endpoint Security tab</th>
<th>The administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td>Read Only</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

|          | No | • Save and Install buttons are disabled. |
|          |    | • The administrator can only be assigned Remote Help access permissions by an administrator with full access. |

### Remote Help

<table>
<thead>
<tr>
<th>Object Database</th>
<th>The administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td></td>
</tr>
<tr>
<td>Read Only</td>
<td>• Cannot create, modify, or delete Security Management Server objects, either from SmartDashboard or the Endpoint Security Management Console.</td>
</tr>
<tr>
<td></td>
<td>• Gives remote help for:</td>
</tr>
<tr>
<td></td>
<td>• User Preboot logon</td>
</tr>
<tr>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
</tbody>
</table>
Chapter 3

Endpoint Security Licenses

Licenses are installed on the Endpoint Security Management Server.

In This Chapter

- Endpoint Security License Types
- Demo and Product Licenses
- License Behavior
- Getting Licenses
- Getting and Applying Contracts
- License Status

Endpoint Security License Types

Endpoint Security requires these licenses:

<table>
<thead>
<tr>
<th>License Type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container license</td>
<td>A one-time license for the Endpoint agent. Each endpoint requires a container license.</td>
</tr>
<tr>
<td>Software Blade licenses</td>
<td>A license for each Endpoint Security Software Blade, such as Full Disk Encryption, Media Encryption &amp; Port Protection, WebCheck, and Network Protection (a single blade consisting of Firewall, Endpoint Compliance, Application Control, and Anti-Malware.) Each endpoint requires a license for each blade that is installed on it.</td>
</tr>
<tr>
<td>Management license</td>
<td>A license for the Endpoint Security management itself. The management license includes 3 blades: Management, Logging &amp; Status, and User Directory. Choose from the pre-defined license systems based on the number of endpoints that you manage.</td>
</tr>
<tr>
<td>VPN License</td>
<td>A license for the VPN gateway that Endpoint Security users connect to. Install it on the Security Management Server that manages the VPN gateway, NOT on the Endpoint Security Management server.</td>
</tr>
</tbody>
</table>

Demo and Product Licenses

These Endpoint Security licenses are available:

<table>
<thead>
<tr>
<th>License type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plug and Play</td>
<td>A 15 day demo license is automatically installed with Endpoint Security software. The Plug and Play license provides use of all Endpoint Security software blades for a predefined number of seats.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>An evaluation license is available for specified software blades for a predefined number of seats.</td>
</tr>
</tbody>
</table>
License Behavior

License activity conforms to these conditions:

- Endpoint Security licenses are added either from SmartUpdate or from the Command Prompt window with the `cplic` command. Install the license for the first time with the `cplic` command.
- Every client gets specified licenses from the pool of available licenses. Each client has a container license and a license for each Software Blade. Floating licenses are not supported.
- You can combine licenses to reach the total number of required clients.
- License validation occurs when the client sends either a SYNC or heartbeat messages to the server.
- License expiration dates of the Endpoint Security Software Blades are downloaded to the client.
- License deactivation is supported through the Endpoint Security Management Server console.
- When there is no container license, software blade registration is blocked.

Getting Licenses

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

To get the license for your Endpoint Security Management Server:
1. Log in to Check Point User Center (http://usercenter.checkpoint.com).
2. Click Products.
   - The page shows the purchased licenses.
   - Endpoint Security licenses have these parts in the SKU:
     - CPEP - Check Point Endpoint Security containers.
     - CPSB - Check Point Software Blade. If the Macro string includes the -SUBSCR suffix, you must get and apply a contract for this feature ("Getting and Applying Contracts" on page 32).
3. For each license, select License in the drop-down menu at the right of the row.
4. Fill in the form that opens.
   - Make sure that Version is R80 and above.
   - Make sure that the IP Address is the IP address of the Endpoint Security Management Server.
5. Click License.
   - A window opens, showing the license data.
6. Copy the Run command, without the single- quotation marks.
   - This is the license command with your license key.
7. On the Endpoint Security Management Server, run this command.

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 access to the Internet, download the contract directly to its file system.

To apply a contract:
1. Log in to Check Point User Center (http://usercenter.checkpoint.com).
License Status

On the Overview tab, you can view license details and status in the License Report area.

To show license details:
1. In the License Report area, click View By License. The License section is displayed.
2. Click the license identification number.
3. Click Show Details to display:
   - License SKU
   - Total seats
   - Expiration date
   - Software blades installed

To show the license status of software blades:
1. In the License Report area, click View By Blade.
2. The Blade section displays:
   - Maximum number of clients supported by each blade license.
   - Number of current clients by blade license.
   - Number of clients that are about to expire by blade license.

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)
6. Select **License & Contracts** > **Updated Contracts** > **From File**.
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 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.
Deployment Overview

The first step in deploying client packages is to decide which Software Blades you want to deploy in your organization. Then define profiles that contain the Software Blades (on page 11) that you want to deploy.

There are two basic ways to distribute the client packages:

- Using Software Deployment Assignments
- Deploying an exported package

The Endpoint Security client packages are usually installed in 2 stages:

- **The Initial Client** - This contains the Endpoint Agent, the basic infrastructure for the client to communicate with the Endpoint Security Management server and the container for a Software Blade package.

- **A selected Software Blade Package** - The Software Blades that you install on the client. You can select to include all blades or only specified blades.

You can deploy the Initial Client and the Software Blade package in one file, but administrators usually deploy them separately in this sequence:

1. Distribute the initial client.
2. Confirm that the installation succeeded and the client can communicate with the Endpoint Security Management server.
3. Distribute the Software Blade package.

**Note** - Users must have administrator rights on their computers to install the Endpoint Security msi packages.

The Initial Client

The Initial Client has a version for Windows 32-bit and a version for Windows 64-bit. However you can install the 32-bit version on endpoint computers that run 32 bit or 64-bit Windows versions.

We recommend that you get the Initial Client from the Endpoint Security Management Console because after installation, it connects to the server automatically.
If you get the Initial Client from the installation CD or Check Point website, you must give users the name or the IP address of the Endpoint Security Management server. They must enter this information to connect to the Endpoint Security Management server after installation.

Summary of how to get and distribute the Initial Client:

<table>
<thead>
<tr>
<th>Get it from</th>
<th>What to do:</th>
<th>What users will do</th>
</tr>
</thead>
</table>
| The Endpoint Security Management Console | • In the Endpoint Security Management Console, go to the **Software Deployment** tab.  
• Click **Get Initial Client**  
• Distribute to users using third-party distribution software or other method. | If the distribution method does not install the file silently, users double-click the file to start the installation.  
The client automatically connects to the Endpoint Security Management server. |
| The installation CD                 | • Get the NEWDA file from CD2 of the Endpoint Security installation package.  
• Distribute to users using third-party distribution software or other method. | If the distribution method does not install the file silently, users double-click the file to start the installation.  
After the installation users must enter the name or IP address of the Endpoint Security Management server to connect to it. |
| The Check Point Support Center       | Tell users to download the Initial Client from the Check Point Website (http://supportcenter.checkpoint.com/file_download?id=12168). | Users download the MSI file, and double-click it to start the installation.  
After the installation users must enter the name or IP address of the Endpoint Security Management server to connect to it. |

Getting the Initial Client from the Console

Here are detailed instructions of how to get the Initial Client from the Endpoint Security Management Console.

The Initial Client and the Software Blade package both have the filename, EPS.msi. You must not change the filename. To identify each EPS.msi file, create a new folder with a descriptive name for each package. For example, when you save the Initial Client package in this procedure, you can make a folder called "Initial Client for 32 and 64 bit".

**To get the Initial Client:**

1. In the Endpoint Security Management Console, go to the **Software Deployment** tab.
2. Click **Get Initial Client**.
3. In the **Platform Selection** window, select  **Windows 32-bit Versions**.
   * The Initial Client for 32-bit, is supported on 32-bit and 64-bit systems. You can deploy that one Initial Client to all endpoint Windows computers, regardless of their exact operating system.
   * If you deploy the 64-bit client on a 32-bit system, installation will fail.
4. Click **OK**.
5. In the **Uninstall Password** window, click **OK** (unless you are upgrading a pre-R80 installation).
6. In the **Browse for Folder** window, click **Make New Folder** and give the folder a descriptive name, such as "Initial Client for 32 and 64 bit".
7. Click **OK**.
   * The client downloads to the specified location. This can take a long time.

Distributing the Initial Client

Distribute the EPS.msi file to all endpoint computers. You can use third-party distribution software, email with shared network path, or another distribution method to distribute it.

- If you use third-party distribution software to install the file silently, the client connects to the Endpoint Security Management server automatically and users do not do anything.
The Software Blade Package

- If you distribute the file to users, they double-click it to start the installation. When the installation completes, the client connects to the Endpoint Security Management server automatically.
- If you get the file from the Installation CD or if users get it themselves from the Check Point Support Center, they must enter the name or IP address of the Endpoint Security Management server to connect to the server after the installation. Make sure to give them this information.
- An msi file that contains only an Initial Client cannot be installed on a computer that already has a client installed.

Seeing the Deployment Status

See the status of the deployment in the Endpoint Security Management Console:
- A summary in the Software Deployment tab > Initial Client Package Deployment area. Click the arrow next to Show Report.
- The detailed deployment status in Monitoring tab. Select Software Deployment from the tree.

The Software Blade Package

The Software Blade package contains the Software Blades that will be on the client.

Each Software Blade has one or more policies that contain its settings. You can configure policies for the Software Blades in the Endpoint Security Management Console before you distribute the Software Blade package or afterwards.

A Profile contains two Software Blade packages, one for 32-bit systems and one for 64-bit systems. A profile also contains global properties and settings.

The standard packages are:

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

Summary of how to distribute Software Blade packages and subsequent updates:

<table>
<thead>
<tr>
<th>Method</th>
<th>What to do</th>
<th>Advantages/Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Deployment Assignments</td>
<td>• In the Software Deployment tab, create a new Profile or select an existing profile.</td>
<td>The Endpoint Security Management server automatically distributes 32-bit packages to 32-bit systems and 64-bit packages to 64-bit systems. You can see the status of all deployments in the Monitoring tab.</td>
</tr>
<tr>
<td>(&quot;Distributing with Assignments&quot; on page 39)</td>
<td>• Click Assignments.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add all nodes on which you will install the package.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Install Policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export Package</td>
<td>• In the Software Deployment tab, create a new Profile or select an existing profile.</td>
<td>You must make sure to install the 32-bit package on 32-bit systems and the 64-bit package on 64-bit systems. If you distribute the wrong package, the installation fails. You can only see the status of deployments that have successfully installed the package.</td>
</tr>
<tr>
<td>(&quot;Distributing by Exporting the Package&quot; on page 40)</td>
<td>• Click Export Package.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Choose 32 or 64 bit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Save the package to a directory and distribute it to users as you choose.</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Basic Package

In the Software Deployment tab, you configure a Profile. A Profile contains two Software Blade packages, one for 32-bit systems and one for 64-bit systems. A profile also contains global properties and settings.

To configure a Profile:
1. Open Software Deployment > Overview.
2. In the Configure and Deploy Software Blades section, click New. The Software Deployment Profile window opens.
3. In the General Properties pane:
   • Enter a name for the profile object
   • Optionally, select a color and add a comment to identify this set of deployment settings
4. Select the blades to include in the profile packages. The smallest package that contains those blades is put in the profile. 32-bit and 64-bit packages are included.
5. You can see the exact name and version of the included packages in:
   • 32-bit Package- Select Package Settings from the tree.
   • 64-bit package- Select 64-Bit Support from the tree.
6. Click OK.

You can include different packages than the automatically selected ones or add HFAs or Hotfixes.

To change the packages in a profile:
1. In an open profile, select Package Settings from the tree.
2. In the Base Package area, click Select and choose a package. The Manage Packages window opens.
3. Select a package from the Available Packages and click OK. This is the 32-bit package.
4. If the Endpoint Security client packages are stored in a non-default location, click Add From File, browse to the relevant package, and click OK.
5. Select 64 Bit Support from the tree.
6. Select a package from the Available Packages and click OK. This is the 64-bit package.
7. If the Endpoint Security client packages are stored in a non-default location, click Add From File, browse to the relevant package, and click OK.
8. Click OK.
9. Click OK.

Client Packages on the Installation CD

CD2 of the installation CDs contains Endpoint Security client packages.

<table>
<thead>
<tr>
<th>Directory Name on CD</th>
<th>Package description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master_EVAL</td>
<td>Evaluation mode client, 32 and 64 bit versions</td>
</tr>
<tr>
<td>Master_EVAL_x64</td>
<td></td>
</tr>
<tr>
<td>Master_FULL</td>
<td>Full package, 32 and 64 bit versions. This includes all blades</td>
</tr>
<tr>
<td>Master_FULL_x64</td>
<td></td>
</tr>
<tr>
<td>Master_FULL_NO_NP</td>
<td>Check Point Media Encryption &amp; Port Protection, Full Disk Encryption, and WebCheck</td>
</tr>
<tr>
<td>Master_FULL_NO_NP_x64</td>
<td></td>
</tr>
<tr>
<td>NEWDA</td>
<td>Initial Client, 32 and 64 bit versions</td>
</tr>
<tr>
<td>NEWDA_x64</td>
<td></td>
</tr>
</tbody>
</table>
Global Package Configurations and Content

The global package settings that are configured take effect when you export or assign a package. The global settings that you can configure are:

- Which certificate Authority signs client packages
- A default VPN site that users will connect to.

To see the Global Package Settings:
1. Open Software Deployment > Overview.
2. If the Global Packages Configurations and Content pane is not visible, from the View menu select Software Deployment Overview > Global Packages Configurations.
3. See how packages are signed and if a VPN site is defined.

Configuring Software Signatures

You can make sure that remote endpoints of your organization receive the correct MSI package by adding a signature to the client package. The certificate is kept on the server and authenticated by the endpoints.

By default, an internal signature is created.

To create a custom signature:
1. In the Software Deployment tab, go to the Software Signatures page in one of these ways:
   - In the Global Package Configuration and Content pane, see Packages are being signed by the internal CA, or a different signature status and click Go.
   - In the tree in the left pane, go to Advanced Package Settings > Software Signature.
2. In the Certificate Settings options, select Custom.
3. Browse to the certificate (P12 file) to use.
4. Enter a name and password for the certificate.
   The certificate is created on the Endpoint Security Management Server. Copy this file and send to client computers before you install the client on them.

Configuring a Client Package with a Default VPN Site

You can configure Endpoint Security clients to be able to connect to a default VPN site. This is useful if your organization has an option to connect through VPN, especially on laptops. To enable clients to use VPN, the Endpoint Security client packages that you configure must include a VPN blade.

Note - When creating a Software Deployment client package, you can select which remote access client should run by default on the endpoint. When selecting the Firewall blade, for example, the legacy remote access VPN client is selected by default. However, the Remote Access VPN client can be selected in addition to the legacy VPN client so that the package contains both clients.

When exporting the package, you are asked to select the default client of your choice.

To configure a client package with a default VPN site:
1. In the Software Deployment tab, go to the VPN Client Settings page in one of these ways:
   - In the Global Package Configuration and Content pane, see the VPN status and click Go.
   - In the tree in the left pane, go to Advanced Package Settings > VPN Client Settings.
2. Click New.
   The Endpoint Secure Configuration window opens.
3. Enter the VPN Site details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>A name for the VPN site, to be seen by users of clients and by system</td>
</tr>
<tr>
<td></td>
<td>administrators.</td>
</tr>
</tbody>
</table>
Distributing Software Blade Packages and Updates

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site address</td>
<td>The DNS name or IP address of the Security Gateway that provides remote access to the corporate network.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Select your method of authentication to the VPN.</td>
</tr>
</tbody>
</table>

### Authentication Method

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name-Password</td>
<td>Username and password that will authenticate users to the VPN; make sure the Endpoint Connect administrators have the list of users who will have the client installed and that the users get their VPN passwords.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Make sure users get a copy of the certificate created by Endpoint Connect.</td>
</tr>
<tr>
<td>SecurID</td>
<td>Make sure the users get the Key FOB hard token, PinPad card, or SecurID Software token, and the necessary information to authenticate the selected key type.</td>
</tr>
<tr>
<td>Challenge Response</td>
<td>Make sure the users get the string they must supply as a response to the VPN authentication challenge.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

### Distributing Software Blade Packages and Updates

There are two primary ways to distribute the Software Blade package and all updates afterwards

- **Software Deployment Assignments** - All packages other than the initial client can be distributed this way. It is fully managed by the Endpoint Security Management server.

- **Exporting Packages** - All packages can be distributed this way. Export the package from the Endpoint Security Management Console and distribute it with a third party, such as GPO, or email to a shared server.

### Distributing with Assignments

Software Deployment Assignments lets you fully manage package distribution and updates with the Endpoint Security Management Console. You select active directory nodes and easily distribute packages to those nodes.

After the Initial Client is installed on a computer, the system architecture (32-bit or 64-bit) is detected and the correct package is automatically deployed. This is a big advantage over other distribution options, as the administrator does not have to know exactly which system architecture each computer has.

You can monitor all stages of the installation in Monitoring > Software Deployment.

You must install an Initial Client on computers before you can use Assignments, as the Assignments require communication between the Endpoint Agent and the Endpoint Security Management server.

**To assign a Profile:**

1. In the Software Deployment tab, in an open profile, select **Assignment** from the tree.
   
   You can see all modes that have the policy assigned.

2. Click **Add Assignment**.
   
   The **Select Node** window opens.

3. In the **Select Node** window, select a node from the Active Directory. Each node represents an object in the organizational tree.

4. Click **OK**.

5. Select **File > Install Policies** or click the **Install Policies** icon.
Distributing by Exporting the Package

Each Profile contains two packages. The Export Package operation exports one package at a time. It creates a single EPS.msi file that users can double-click to install. This file is either for 32-bit or 64-bit systems, based on the selection you make when you export the file. If you install a package that does not match its system, the installation fails.

Notes on exported packages:
- Double-clicking the MSI does not uninstall the client if the client is already installed.
- The MSI file name must remain EPS.msi. If the file name changes, upgrading or adding a blade or attempts to uninstall the client will fail. You can save each msi file in a different folder with a descriptive name to prevent confusion.
- You cannot manually add a blade to an existing client installation by double-clicking the msi file. To add a blade, use the command line options.

To export a package:
1. In the Software Deployment tab, select a Profile.
2. Click Export Package.
3. In the Platform Selection window, select which package to export from the profile:
   - Windows 32-bit Versions
   - Windows 64-bit Versions
4. Click OK.
5. In the Legacy Uninstall Password window, click Skip (unless you are upgrading a pre-R80 installation).
6. In the Add Virtual Group Destination window, browse to the virtual group for this package. See Virtual Directory Structure.
7. A message shows asking you if you want to override the default VPN client settings configuration. Click No.
8. In the Browse for Folder window, click Make New Folder and give the folder a descriptive name, such as, "32-bit full package."
9. Click OK.
   - The file downloads to the specified location. This can take a long time.
10. Distribute the EPS.msi file to all endpoint computers with that Windows platform. You can use third party distribution software, email with shared network path, or another distribution method to distribute it.
11. Repeat the procedure to create a package for a different Windows platform.

Configuring VPN Client Settings

In an exported package, you can override the default VPN client settings and configure the package to use a VPN site that you select.

To create VPN client settings for a package:
1. In the Software Deployment tab, select a Profile.
2. Click Export Package.
3. In the Platform Selection window, select which package to export from the profile:
   - Windows 32-bit Versions
   - Windows 64-bit Versions
4. Click OK.
5. In the Legacy Uninstall Password window, click Skip (unless you are upgrading a pre-R80 installation).
6. A message displays asking you if you want to override the default VPN client settings configuration.
7. Click Yes.
8. The VPN Client Settings window opens.
9. If you are using Endpoint Connect (Remote Access VPN):
   a) Select Override Endpoint Connect configuration.
b) Select either Manual settings or Import from file.
   (i) If you select Manual settings, select a VPN site from the drop-down list, and click OK.
   (ii) If you select Import from file, browse to the configuration file you want to use, and click OK.

10. If you are using Secure Client (Legacy Client):
   a) Select Override Secure Client configuration.
   b) Browse to the secure client configuration file you want to use.
   c) Select the VPN Client to be used by default in the package from the drop-down list.

Installing the Client Using the CLI

You can install an exported package with the CLI on a client computer. Use these commands:

<table>
<thead>
<tr>
<th>Command line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msiexec /i &lt;path to EPS.msi&gt;</td>
<td>Do a fresh installation</td>
</tr>
<tr>
<td>msiexec /i &lt;path to EPS.msi&gt;</td>
<td>Add an initial blade or blades</td>
</tr>
<tr>
<td>msiexec /i &lt;path to EPS.msi&gt; REINSTALL=DUMMY REINSTALLMODE=voums</td>
<td>Add or remove blades</td>
</tr>
<tr>
<td>msiexec /i &lt;path to EPS.msi&gt;</td>
<td>Upgrade using the indicated package.</td>
</tr>
</tbody>
</table>

Logging Options

To create logs, do one of the following:

- Add /l*vd <path to log file> to any of the command lines above.
- Add logging instructions to the Windows's 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>voicewarmupx</td>
<td>windows generates the log file under the %TEMP% directory, and names it MSI*****.LOG.</td>
</tr>
</tbody>
</table>

Troubleshooting the Installation

Administrative Privileges

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

- Installing or uninstalling the client on Windows 7 or Vista with active UAC (User Access Control) requires the user to invoke the installer with the "run as administrator" option. To enable this right-click mouse option, add the following information to the registry:
To install or uninstall using the command line, the user must have administrator privileges ("run as administrator").

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

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

Microsoft suggests two possible solutions:

<table>
<thead>
<tr>
<th>Microsoft Solution</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB311269</td>
<td>Register the WScript object by running the <code>wscript -regserver</code> command from a command prompt or from the Run option on the Start menu.</td>
</tr>
<tr>
<td>KB20027</td>
<td>Make sure Scrrun.dll is installed on the endpoint computer, and that it is correctly registered. To register the dll:</td>
</tr>
<tr>
<td></td>
<td>• Open a command prompt</td>
</tr>
<tr>
<td></td>
<td>• Change directory to <code>c:\windows\system32</code></td>
</tr>
<tr>
<td></td>
<td>• Run: <code>Regsvr32 scrrun.dll</code></td>
</tr>
</tbody>
</table>

See also DES encryption on Windows 7 clients ("Configuring Active Directory for Authentication" on page 45)

**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
```

**Client logging**

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

- Firewall
- Application Control
- Anti-malware
- Endpoint Compliance
- Full Disk Encryption
- Media Encryption and port protection
- WebCheck

On the server, the logs are stored in the common log database, which is read by SmartView Tracker.

**Note** - The VPN blade does not upload logs to the server.
Client logs are:

- Stored locally at:
  
  ```
  C:Documents and SettingsAll UsersApplication DataCheckPointEndpoint
  SecurityLogs
  ```

<table>
<thead>
<tr>
<th>Log File</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>epslog.1.log</td>
<td>Clear text logging file</td>
</tr>
<tr>
<td>epslog.2.log</td>
<td>When the file becomes too large, another is created.</td>
</tr>
<tr>
<td>epslog.&lt;number&gt;.log</td>
<td>Maximum of 10 log files can exist. When epslog.11.log is created,</td>
</tr>
<tr>
<td></td>
<td>eplog1.log is deleted.</td>
</tr>
<tr>
<td></td>
<td>Can be viewed with any ASCII viewer, or by using the client</td>
</tr>
<tr>
<td></td>
<td>viewer, or by manually running:</td>
</tr>
<tr>
<td></td>
<td>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>

- 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 Endpoint Security User Guide (http://supportcontent.checkpoint.com/solutions?id=sk65376) for detailed information about what clients can do with logs on their computers.

### Uninstalling the Client

The client can be uninstalled using:

- **Add/Remove Programs** applet in Control Panel
  - Before uninstalling:
    - On Windows 7, turn off User Account Control (UAC).
    - Make sure the original EPS.msi file still resides locally on the computer.
  - If the client had the Full Disk Encryption blade enabled, after the disk finishes decrypting, run the **Add/Remove** applet again.

### Evaluation Mode Client

On CD2, in the MSI > Master_EVAL folder, Check Point provides a predefined client (EPS_Evaluation.exe) for evaluation purposes.

Do a typical installation, evaluating all the features or blades, or do a custom installation where only selected blades are installed. The central difference between the regular client and the evaluation mode client is the lack of a server connection.

**Note** - Do not rename the installation package before installing it.
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 Endpoint Security Management Console 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.

### Table: Blade or Feature vs Comments

<table>
<thead>
<tr>
<th>Blade or Feature</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Network Security Features   | • Firewall Rules  
  • Endpoint Compliance  
  • Application Control  
  • Malware Protection  
  All function the same as in the full production client but using the default policies.                                                                 |
| Full Disk Encryption        | During the installation, you have to decide between:  
  • Encrypt all disks with a fixed key  
  • Do not encrypt any disk  
  If you decide to encrypt, the hard drive is encrypted using AES 236-bit for 15 days. After 15 days evaluation, the disk decrypts.  
  If you need to recover the disk, either:  
  • Use the **recovery** option available by pressing the shift key twice prior to pre-boot  
  • Do normal recovery using the recovery.iso file on CD2 in the **Tools** folder |
| Media Encryption and Port Protection | No interaction with an Endpoint Security Management Server means that there is no central key storage on the server, and therefore no automatic access to encrypted media. To access encrypted media, the user must enter a password. |
| Remote Access VPN           | Behaves the same as in the production client. Licenses are enforced by the gateway.                                                                                                                      |
| WebCheck                    | Behaves the same as in the production client, but uses the default policy.                                                                                                                                |

**Note** - The evaluation mode client cannot be turned into a full production mode client. In the notification area, there is no right-click menu option available for entering the IP address of the server.
This option is available for endpoints that are part of Active Directory.

**Figure 4-2** Endpoint Security Authentication Process

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 switch 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** - After you configure your Endpoint Security Management Server to work only with authenticated clients, client computers that do not belong to an Active Directory will not function correctly. This is because they cannot send authenticated messages.

**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 clients that they now work in Authenticated mode.

**Configuring Active Directory for Authentication**

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

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

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

To prepare the Active Directory Server for authentication:
1. Run ktpass.exe.
2. Go to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
3. Create a domain user and clear the **User must change password at next logon** option.
4. Run this command to map a service to a user:
   **Syntax:**
   ktpass princ ServiceName/realm@REALM mapuser <userName>@REALM pass <userPass> out <name of outFile>
   **Example:**
   ktpass princ tst/nac1.com@NAC1.COM mapuser auth-user@NAC1.COM pass 123456 out outfile.keytab
   **Where:**
   ServiceName= tst
   realm (domain name)= NAC1.COM (in princ command: the first time in lower case and the second in upper case)
   userName = auth-user (user from item 4)
   userPass = 123456 ( password for user from item 4)
   name of outFile = outfile.keytab = encrypted keytab file
5. Save the console output to a text file. See the version number (vno) and encryption type (etype).
   **Sample output:**
   Targeting domain controller: nac1-dc.nac1.com
   Successfully mapped tst/nac1.com to auth-user.
   WARNING: pType and account type do not match. This might cause problems.
   Key created.
   Output keytab to outfile.log:
   Keytab version: 0x502
   keysize 74 tst/nac1.com@NAC1.COM ptype 0 (KR5_NT_UNKNOWN) vno 7 etype 0x17 (RC4-HMAC) keylength 16 (0x32ed87bd5fda59cb8547376818d4)

**Important** - We recommend that you do not use DES-based encryption for the Active Directory Domain Controller server, as it is not secure. If you choose to use DES encryption and your environment has Windows 7 clients, see sk64300 (http://supportcontent.checkpoint.com/solutions?id=sk64300).

### Configuring Authentication Settings

To set up Strong Authentication, configure the **Authentication Settings** of a package profile.

**Important** - Remember to use Unauthenticated mode while evaluating only; it is not intended for production environments. Set up authentication just before moving to production.

**To configure authentication settings:**
1. In the Endpoint Security Management Console open **Manage > General Properties > Authentication Settings**.
   The **General Properties** window opens.
2. Click **Authentication Settings**.
3. Click **Add**.
   The **Active Directory SSO Configuration** window opens.
4. Enter the details of the configured Active Directory, taken from the output of the Active Directory map service command.

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

5. Click OK.
6. When you are ready to work in Authentication mode, select Work in authenticated mode in the Authentication Settings pane.

When you configure client package profiles, you will have to choose an authentication account. The SSO Configuration details will be included in the client package, allowing the server to authenticate the client.

**Important** - After turning on Strong Authentication, wait one minute before initiating any client operations.

It will take time for the clients and the Endpoint Security Management Server to synchronize. During this time, the environment will remain unauthenticated, and some operations will fail. The exact amount of time depends on the synchronization interval ("Directory Synchronization" on page 26).

### Troubleshooting Authentication in Server Logs

To troubleshoot problems related to active directory Authentication, use the Authentication log on the server in %uepmdir%/logs/Authentication.log.

**To see full debugging information in the Authentication.log file:**
2. In the Advanced tab, click Environment Variables.
3. Select the variable TDERROR_ALL_KERBEROS_SERVER and click Edit.
4. Change the value of the variable to 5.
5. Click OK.
6. Click OK.
7. Restart the Apache Server.

If the Authentication.log file on the server shows:

```plaintext
ERROR: Config file contains no principals.
```

The database was cleaned or the process to include authentication in the client package was faulty. To fix:
1. Repeat the process to configure authentication ("Configuring Authentication" on page 45).

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

Restart the Apache service on the Endpoint Security Management Server: `apache -k restart`.

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/config/global.properties`, add this line:

```
authentication.clockSkew.secs=<seconds>, where you replace <seconds> with the clock skew in seconds that you want to allow.
```

If the **Authentication.log** file on the server shows:

Key version number for principal in key table is incorrect

Update the **Key version number** in the **Active Directory SSO Configuration** window. You might have changed the user that is mapped to the ktpass service ("Configuring Active Directory for Authentication" on page 45).
Chapter 5

Upgrading Clients

In This Chapter

Upgrading Clients to this Version 49
Upgrading Legacy Clients 50

Upgrading Clients to this Version

Earlier versions of R80 clients can be successfully upgraded to R80.x or E80.x versions, if:

- The entire MSI package is upgraded together. This includes the Endpoint Agent and Software Blades. You cannot upgrade only the Endpoint Agent.
- The upgraded Software Blades must have the same configurations as before. To upgrade and change the configuration, upgrade to the same configuration first and then add or remove blades.

After you upgrade all servers, deploy new client packages. The workflow is:

- Upgrade the Profiles.
- Distribute the profile packages automatically or with an exported package.

Upgraded clients and non-upgraded clients can connect to the same upgraded server.

Upgrading with Assignments

The Common 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 Common Client Policy > General Properties > Client Install / Uninstall Settings.

To upgrade clients with Software Deployment Assignments:
1. In the Software Deployment tab, select a package and click Upgrade Profile.
   A message opens that shows if an update is available.
2. Click Yes to confirm that you want to upgrade the profile.
   All computers who are assigned to that profile will be upgraded.
3. Optionally, click Assignments to edit the assignments of the profile.
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 Common Client Settings Settings policy control.
   - If the Common 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.

   Endpoint Security Client is attempting to accept an upgrade.
   During this installation all remote VPN connections will be terminated and your computer will restart.
   Save your work before installation starts.
   Do you want the installation to start now?
   If you choose No, installation will start automatically at HH:MM
6. The Endpoint Agent installs the new client.
Installation starts automatically after a timeout if the user did not click Yes.

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 Software Deployment tab, select a package and click Upgrade Profile. A message opens that shows if an update is available.
2. Click Yes to confirm that you want to upgrade the profile.
3. Do the procedure to export a package ("Distributing by Exporting the Package" on page 40).

**Upgrading Legacy Clients**

See the Endpoint Security Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk65376) for the supported upgrade paths for this version. There are different procedures for offline and online.

- Offline - The endpoint has no connection with the Endpoint Security Management server.
- Online - The endpoint can connect with the server.

If you have an earlier version of Full Disk Encryption or Full Disk Encryption MI, see Upgrading Legacy Full Disk Encryption (on page 98).

**Offline Upgrades**

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

- All the passwords necessary to successfully uninstall legacy products
- The new E80.20 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 Software Deployment tab, click New.
2. The Software Deployment Profile window opens.
3. Create a profile with the needed blades.
4. Click OK.
5. Select the new profile in the table, and click Export Package. The Uninstall Password window opens.
6. In the Legacy Upgrade area, select Support legacy upgrade and enter the passwords needed to uninstall legacy products.
7. In the FDE Update Validation Password area, select Support legacy upgrade and enter the passwords used in legacy EW Full Disk Encryption. This is required for EW Full Disk Encryption to upgrade to the latest version.
8. Click OK.
9. Browse to the location that the package will export to.
10. Click OK. The package exports to the chosen location. The Preupgrade.exe file is automatically created in the same directory.
11. Supply the Preupgrade.exe file to the offline endpoints.

**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 Policy** that contains uninstall passwords for legacy products.

**To create a package for an Online upgrade:**

1. In the **Policies** tab > **Common Client Settings Policy Overview**, select **Initial Common Client Policy**.
2. Click **Edit**.
   - The **Common Client Policy** window opens.
3. Click **Legacy Client Uninstall Password**.
4. Enter uninstall passwords for:
   - Legacy Secure Access
   - Legacy FDE EW
5. Click **OK**.
6. On the **Software Deployment** tab, **export an Endpoint Security Agent package**.
7. The **Uninstall Password** window opens giving you a chance to change the uninstall passwords.
8. Click **Skip**.
9. Browse to a folder and save the Endpoint Security Agent package.
10. Deploy the client package to endpoints.
Chapter 6

Using the Endpoint Security Management Console

Use the Endpoint Security Management Console, 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 of the Endpoint Security Management Console.

To open the Endpoint Security Management Console:
Go to Start > All Programs > Check Point SmartConsole <version> > Endpoint Security Management.

In This Chapter

Overview Tab 52
My Organization Tab 53
Policies Tab 55
Monitoring Tab 55
Software Deployment Tab 58
Finding Components in the Console 58

Overview Tab

The overview tab provides a general summary of your Endpoint Security deployment.
<table>
<thead>
<tr>
<th>Area</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Policies | Shows the number of policies in use for:  
  - Software Deployment  
  - OneCheck User Settings  
  - Full Disk Encryption  
  - Media Encryption & Port Protection  
  - Access Zones  
  - Malware Protection  
  - Firewall Rules  
  - Application Control  
  - Endpoint Compliance  
  - WebCheck  
  - Common Client Settings |
| Monitoring Summary windows 1 and 2 | Shows the current status of your endpoints according to user selectable types of status information.  
**Browse** button (not available for all report types) lets you filter the summary according to individual user object nodes or groups of nodes.  
**Show Details** Shows a detailed view of the selected portion of the report. Sort the view according to specific columns.  
Use the (+) sign in the title bar to clone the monitoring window any number of times. |
| License Reports | View license reports either by License or by Blade. If viewed by license, purchased licenses are shown in the bar chart. View more details of the selected license by clicking **Show Details**.  
If viewed by Blade, the number of licensed seats available is shown per blade. Each bar represents the accumulation of all licenses purchased for the specified blade. |
| Getting Started | Shows a checklist of tasks for quickly deploying Endpoint Security Clients, and links to the relevant pages and windows. Selecting each task strikes it from the list |
| Endpoint infections | Provides a summary of infections during the last twenty-four hours. |
| Anti-Malware Updates | Shows the anti-malware version currently deployed, and lets you check for available updates. |

Use the **View > Endpoint Management Overview** option to control which areas of the tab are shown.

**My Organization Tab**

This tab shows your environment in a hierarchy organization (tree structure) model where your AD server information is displayed. Use the **My Organization** tab to manage the security of endpoint computers via the active directory objects (Organizational Units (OUs), groups, computers, and users).

Under the **My Organization** root are three top-level nodes:
### Node | Purpose
--- | ---
Directories | After scanning an Active Directory, this node is populated with the Active Directory tree structure. The middle pane of the My Organization tab displays the list of groups, users, and computers in the folder or group.

*<domain name>_All Groups* - Contains all groups found by the directory scan. The groups are displayed both where they occur in the tree structure and in this special container.

Networks | Networks organized by IP range

Other Users/Computers | Contains:
- All users and computers not found in the Active Directory but which exist on the computer on which the Endpoint Security client is installed.
- Objects that have been deleted from the Active Directory but whose recovery information is retained for possible future use.

In addition to the AD tree structure, the window is divided into 4 sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Monitoring Summary | Similar to Global Monitoring on the Overview tab. Monitoring Summary shows status information according to report type, the report related to the node selected in the organizational tree.  
*Note:* These reports are not available for users, computers, and AD groups. |
| Software Blades by Computer | Shows the Software Blades installed on the selected profile. You can edit an existing profile, create new profiles, or override the profile completely. |
| Policies Assignment | Lists policy assignment types |
| Comments | Provides space for administration notes |

The Policy Assignment pane shows the configured security policies assigned to the currently selected folder, network, group, computer, or user. A specified user or computer inherits the policies of its parents, unless you directly assign another policy of the same type or other ranking criteria are applied ("Assigning Policies" on page 63).

### Managing Networks

The nodes of the My Organization tree are filled automatically, either by scanning the Active Directory or by installing the Endpoint Security client. The only node whose contents you define and manage is the Networks node.

**To create a My Organization Network:**

1. Open the My Organization tab.
2. Right-click Networks and select New Address Range. The Address Range Properties window opens.
3. Provide a name to identify this address range as a managed network.
4. Provide the first IP address and the last IP address of the range.
5. Add a descriptive comment, and select a color.
6. Click Save.
Policies Tab

On the Policies tab, you define and manage policies for each Endpoint Security Software Blade. An **Endpoint Security policy** is a collection of security rules that enforce protections.

The **Policies** tree includes an **Overview** option and the available Software Blades. The pane shows the policies for the selected Software Blade.

If you select the **Overview** option, these tables show in the pane:

- **Policy Assignment Per Blade** - Shows the number of policies assigned or unassigned for each blade.
- **Policy Status** - Shows the modification and deployment status of each policy.
- **Group Assignments Priority** - Shows the priority for assigning policies to groups.

Click **View > Policy Overview > Group Assignment Priority**. Group Assignment Priority (on page 64) lets you configure which groups have higher priority when assigning policies.

Monitoring Tab

The Monitoring 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 the Endpoint Security Management Console, click the **Monitoring** tab.
2. Select a report type from the **Monitoring** tree.
   The report shows in the pane.
3. Double-click the **User** or **Computer Name** fields an item to open a **Details** window that shows additional detailed information. You can also assign, create and change policies from the **Details** window.

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

**Compliance History** - Shows compliance status incidents occurring during the last 24 hours. Click a point in the chart to item the number of active incidents at that time.

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 soon be restricted if action is not taken to make it compliant.
- **Observe** - One or more of the compliance rules that is set as **Observe** is not satisfied. Users are not aware of 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. Take steps to make the computer compliant.
- **Not Available** - The network protection is disabled or not installed.

Activity Reports

The **Activity Reports** group includes these endpoint and policy server status reports:

- **Endpoint Connectivity** - Shows the last time each endpoint computer connected to the network.
• **Endpoint Blade Status** - 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** - Computer 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** - Computer that have the Endpoint Agent installed.

• **Endpoint Policy Server Status** - Shows policy server status (Active or Not Active)

• **Endpoint Connectivity by Policy Server** - Shows which Endpoint Policy Server each endpoint communicates with.

### Software Deployment

You can select reports that show deployment status by:

• **Deployment Status** - Shows deployment by the status category of deployment.

• **Package** - Shows deployment status by package name

• **Profile** - Shows deployment status by profile name

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

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

Hold the mouse above an item in the Legend to highlight it and see the number of endpoint computers in each status category.

### Anti-Malware

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

• **Malware Protection Status** - Shows scanning detection statistics.

• **Top Infections** - Shows the top five infections during the past 14 days.

• **Malware Protection Provider Brands** - Shows scanning status by Anti-Malware provider brand.

• **Malware Protection Scan Date** - Shows status by the last scan date.

### WebCheck

**WebCheck Status** - Shows the current WebCheck monitoring status for endpoint clients. The status categories are:

- Disabled
- Enabled
- Not installed
- User disabled
- All
Full Disk Encryption

- **Full Disk Encryption Status** - Shows the endpoint computer encryption status. The encryption status categories are:
  - Encrypted
  - Decrypting
  - Not installed
  - Unencrypted
  - Encrypting

- **Full Disk Encryption Troubleshooting** - Shows the status of Full Disk Encryption problem resolution by endpoint computer.

- **Preboot Status** - Shows the status of the Full Disk Encryption Preboot on each endpoint computer. The status categories are:
  - Preboot Disabled
  - Preboot Temporarily Disabled
  - Preboot Enabled
  - Not Installed - Full Disk Encryption is not installed on the endpoint.

Media Encryption & Port Protection

This page shows Media Encryption & Port Protection status and device manufacturer according to these device status categories:

- All Devices
- Allowed devices
- Blocked Devices

Double click a device to see where it was used.

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.

- **WebCheck Versions** - Shows the installed version of the WebCheck blade for individual endpoint clients.

Custom

This report type lets you create custom reports that include multiple types of monitoring criteria.

**To create a custom report:**

1. In the Monitoring tab, select Custom > Custom Report.
2. In the Custom Report pane, click Choose monitoring criteria.
3. In the Custom Report pop-up window, double-click monitoring criteria to move them to the Selected Status list.
4. Click OK to close the window.
5. Use the Show Endpoint that list to show data that matches the selected criteria.
6. Use the Status list to create a filter for endpoint computers that show in the Endpoints List.
Licenses Status Report

The Licenses Status Report shows the current 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.

Software Deployment Tab

You use this tab to:
- Configure and deploy software blades to endpoint clients
- Set the clients VPN settings
- Upload packages to the server
- Select the file signing method to protect the integrity of the client package

Finding Components in the Console

You can use a search feature to find components in your environment, such as endpoints, users, directories, and programs.

To find a component:
1. In the Search field tool bar, enter a string to match a component.
2. In the drop-down list, select one of these:
   - Policies Search
   - My Organization Search (to find a computer, user, or directory of computers or users)
   - Application Control Search
   - All - Search everywhere
3. Click Search.
   The Search Results window opens.
4. If the component you are looking for is listed, double-click it.

Note - Alternatively, right-click any user shown on the Monitoring tab and select Edit.
Chapter 7

Managing Policies and Users

Endpoint Security Policies are a set of configurations that define the behavior of Check Point Endpoint Security clients. Use Policies to easily configure Software Blades and to define the system security.

There are general types of policies, each representing a specific Check Point security feature.

Users and Computers, either entered manually or with the Active Directory Scanner, are all seen as objects in the Endpoint Security Management Console. The Active Directory groups and nodes are also objects in the Endpoint Security Management Console.

In This Chapter

- About Policies 59
- Assigning Policies 63
- Deploying Policies 66
- Managing Users 66
- Managing OUs or Groups 67
- Managing Computers 68

About Policies

An Endpoint Security policy is a collection of security rules that enforce a specific type of protection. A policy is enforced by a specific software blade, which must be installed and licensed.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OneCheck User Settings</td>
<td>Defines user-level authentication for Endpoint Security clients with Full Disk Encryption installed.</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>Combines boot protection, preboot authentication and strong encryption to ensure only authorized users are granted access to information stored in desktops and laptops.</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>Protects data stored on the computers by encrypting removable media devices and allowing tight control over computers' ports (USB, Bluetooth, and so on)</td>
</tr>
<tr>
<td>Access Zones</td>
<td>Defines the topology of the organizational network, separating it into Trusted and Internet domains</td>
</tr>
<tr>
<td>Malware Protection</td>
<td>Defines the protection of clients from known and unknown viruses, worms, Trojan horses, adware, and keystroke loggers.</td>
</tr>
<tr>
<td>Firewall Rules</td>
<td>Blocks or allows network traffic based on attributes of network connections.</td>
</tr>
<tr>
<td>Application Control</td>
<td>Restricts network access on a per-application basis, allowing you to restrict network access between a particular application and the defined Access Zones.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Endpoint Compliance</td>
<td>Ensures that protected computers comply with your organization's requirements, and allows you to assign different security levels according to compliance state. For example, non-compliance may result in a remediation message, a warning, or restriction from the network.</td>
</tr>
<tr>
<td>WebCheck</td>
<td>Protects endpoint computers against phishing websites impersonating other websites for malicious purposes.</td>
</tr>
<tr>
<td>Common Client Settings</td>
<td>Defines a common policy for multiple endpoint clients. This lets you deploy and maintain many clients efficiently.</td>
</tr>
</tbody>
</table>
State of Compliance

Policy settings can determine what applications can be installed or run on a computer, what must be installed or running, and what is not permitted.

If an object (for example OU or user) in the organizational tree violates its assigned policy, its compliance state changes, and this affects the behavior of the endpoint.

- The endpoint status is changed to non-compliant.
- The event is logged, and you can monitor the status of the endpoint.
- The action defined in the policy occurs:
  - A warning or remediation message is displayed on the endpoint
  - The endpoints access to the network is restricted.

Non-Compliance

The client receives a compliance policy from the Endpoint Security Management Server that contains a set of compliance rules. If the a user's computer is in violation of a compliance rule, the policy specifies the action that the client does: Observe, Warn, or Restrict. No alerts are shown by the client if the compliance action is 'Observe'. The alert dialog includes a link to perform a Remediation Action.

You can configure alerts in the Endpoint Security Management Console. You can set different alert messages, and even in different languages, for different states. For example:

- Non-Compliance Message - Shown when the client becomes non-compliant.
- Restrict Message - Shown when the client goes into restrict state.

If action must be taken to become compliant, you can choose to configure the policy to auto-remediate or to start remediation when users click the link in the Endpoint Security Main Page. If you configure auto-remediation, you can configure a tooltip to display a message, such as "Remediation in progress".

Enforcing Policies According to States

Endpoint Security enforces policies on computers and users according their current connection and/or compliance state. When you assign a policy, you can select the state or states during which this policy is enforced. By default, policies apply when the client is Connected.

- 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 this state, you generally 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 Rules
  Access Zones
  Application Control

Configuring Policy Enforcement

You can define enforcement for a policy to use one of these scenarios:

- Connected state only (default).
- Connected and Disconnected states.
- Disconnected state only (for computers or users only).
- Restricted state (for non-compliant endpoint computers only).

**To set an assigned policy to Disconnected state:**
1. Select the container object in the My Organization tree.
2. In Policy Assignment while in edit mode, select a policy.
3. Click Add Policy When > Disconnected.
4. Click Install Policy.

**To set an assigned policy to the restricted state:**
1. Select the container object in the My Organization tree.
2. In Policy Assignment, while in edit mode, select Media Encryption & Port Protection, Firewall Rules, Access Zones or Application Control policy.
3. Select Add Policy When > Restricted.
4. Click Install Policy.

**To remove the Disconnected or Restricted state from an assigned policy:**
1. Select the container object in the My Organization tree.
2. In Policy Assignment while in edit mode, select the Disconnected or Restricted state policy you want to remove.
3. Click Remove State Policy.
   The state of the policy is returned to Connected, which is the default policy.

**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. Endpoint computers send "heartbeat" messages to the Endpoint Security Management Server to make sure that the connections are active and that all policies are up to date. The time between heartbeat messages is known as the heartbeat interval ("Configuring the Heartbeat Interval" on page 63).

**To configure the time period that user have before an endpoint computer is restricted:**
1. In the Endpoint Security console, select Manage > General Properties > Connection Settings.
2. In the Out of Compliance section, enter the number of heartbeats.
3. Click OK.

When you configure this time period, we recommend that you give users sufficient opportunity to:
- Save their data.
- Correct the compliance issues.
- Make sure that the endpoint computer is compliant.

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

\[ \text{number of heartbeats} \times \text{heartbeat interval (in seconds)} \times 60 \]

**User Policy or Computer Policy**

Some configurations are defined in the context of a certain User, while others are defined for a certain Computer. For example, the Firewall Rules policy (defines network connections that are allowed and blocked) applies to the user, and will be enforced for certain users on any computer they choose to use.

The Full Disk Encryption policy (defines, among other things, which drives are to be encrypted) applies to the computer. No matter what user logs in to this computer, the encrypted and decrypted drives remain the same.
Configuring the Heartbeat Interval

Endpoint computers send "heartbeat" messages to the Endpoint Security Management Server to make sure that connections are active and that all policies are up to date. The time between heartbeat messages is known 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 heartbeat interval also controls the time that an endpoint client is in the About to be restricted state before it is restricted.

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

Assigning Policies

Endpoint Security clients get policies when the policies are assigned to endpoints.

When you make changes to policies, you must click Install Policies so that the changes can be distributed to the endpoints.

The default policies are those assigned to the My Organization node. A node inherits policies from higher nodes unless it has a different policy assigned to it directly. Computers and Users also inherit the policies from their parent nodes unless they have a different policy assigned to them directly.

Before you install a package on an endpoint you can configure and install policies for that endpoint. In this way you can plan what the client behavior will be when the endpoint security client is installed. If you do not configure and install other policies before you install a package on endpoints, the default policies from My Organization take effect.

**Note** - If an Endpoint Security client is connected to the server and no user is logged on, the policies configured for My Organization are enforced. The configured policies start to work when the user logs on.

Direct Assignment

You can create and assign a policy to an object in the organizational tree; or you can let the user or computer inherit the policy assigned to its parent node.

For example, open My Organization. Click the root (My Organization); in Policy Assignment you can see the Default Policy. If you make no direct assignments of Policies to children directories, networks, computers, or users, they will all get this policy.

**To assign a different policy to an object:**
1. Select the object in the My Organization tree.
2. In the Policies Assignment section, select a policy in the Features column.
3. From the drop-down box in the same row:
   - Click one of the existing policies
   - Click New to create a new one.

**Note** - Remember that some policies are intended for users, and others for computers.
Inherited Assignment

Endpoint Security clients inherit Policies through the hierarchy of container objects in My Organization. A user or computer may be included in more than one container (for example, the user name in the Active Directory and the IP address through a network defined by a range).

Policy Assignment Order

Any container object in the organizational tree may be assigned multiple security configurations from different sources, through inheritance and local overrides.

Precedence is set for different organizational entities:

1. **IP Range Networks** - if an entity falls into a defined network (specified by IP Address Range), it will get the policy assigned to this network (excluding configurations for Software Deployment and Full Disk Encryption, as they define more static settings of the system).
2. **Direct Assignment** - if a User or a Computer is assigned a specific policy, it overrides inherited policies and takes precedence over the following calculations.
3. **Group Ranking** - each group in an Active Directory has a rank. If an entity is in multiple groups, it gets the policy of the highest ranking group.
4. **Directory** - if the entity is in the Active Directory, and the preceding assignments did not apply, it gets the policy of the closest containing Organization Unit (OU) in the Active Directory.
5. **My Organization**, the root of the organizational tree - if the preceding assignments did not give the entity a policy, the entity gets the default policy assigned to the root of the tree.

Group Assignment Priority

When assigning blade policies to Active Directory groups, conflicts can occur if:

- Users or computers belong to multiple groups
- Each group has different policies for its blades

To resolve conflicts, an assignment priority must be set. The Endpoint Security Management Console lets you set two types of Priority Assignment for AD groups:

- Global Group Priority Assignment
- Blade Priority Assignment

*Note* - Blade priority assignment takes precedence over Global priority assignment.

To Set the Global Group Assignment Priority:

1. Open the Endpoint Security Management Console.
2. Open the Policies tab.
   The Group Assignments Priority area opens.
4. From the drop-down box, select Global.
   The table shows the current global priority.
5. Click Change Priority.

*Note* - This option only shows if a policy is already assigned to the group

The Global: Group Assignment Priority window opens.
6. Use the arrow buttons to move a group up or down.
7. Click OK.

The group at the top of the list gets the highest priority.

For example:

- John belongs to the AD Groups, PR and Sales.
- The two groups have different compliance policies.
• In the Group Assignment Priority table, PR is above Sales. Based on the Global Group Assignment Priority, John receives the compliance policies of the PR group, and not the Sales group.

To set a Group Assignment Priority for a Blade:
1. Open the Endpoint Security Management Console.
2. Open the Policies tab.
4. The Group Assignments Priority area shows.
5. In the View By drop-down, select a blade.
6. Click Change Priority.

   Note - This option only shows if the group already has a blade policy assigned.

The Group Assignment Priority window for the blade shows two options.
• Use global group assignment priority to inherit the global priority (default)
• Override global group assignment priority to override the global priority
7. Select Override global group assignment priority.
8. Use the arrow buttons to reorder the groups.
9. Click OK.

The group at the top of the list gets the highest priority. For example:
• John belongs to two AD Groups, PR and Sales.
• The two groups have the Malware Protection blade enabled.
• The PR groups’ Malware Protection blade has a High Security Policy.
• The Sales group has a Low Security policy.
• Group Assignment Priority has Sales above PR in the list.

Based on Group Assignment Priority, John’s Malware Protection blade receives the Low security policy.

Recommendations for Management

Whether your management model is organization-centric or policy-centric, it is recommended that you assign Policies to your most inclusive organizational units first. After you have established your basic security policy assignments in this way, you can make exceptions and overrides.

For example, if you have a financial application for users in your Human Resources group, you can create two Application Control policies: one that allows this application and one that denies it. Assign the policy that denies access to the root and then override that policy on the HR group in the active directory with the policy that allows it.

Assign your Policies in the following order, from the weakest (My Organization) to the stronger (individual computers). Policies assigned to individual computers that precedence over all other policies.

<table>
<thead>
<tr>
<th>Container Object</th>
<th>Assignment Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Organization</td>
<td>Assign a policy to My Organization to provide a high level of security until further policies are created. For efficient maintenance, make sure to include the most common security requirements for your organization. This policy should be the most restrictive because it becomes the default security configuration if:</td>
</tr>
<tr>
<td>• No overriding policy is assigned.</td>
<td></td>
</tr>
<tr>
<td>• The Endpoint Security Management Server cannot resolve a lower container or node.</td>
<td></td>
</tr>
<tr>
<td>• A user logs into a computer for the first time after client installation, and the client cannot connect to the server.</td>
<td></td>
</tr>
</tbody>
</table>
### Container Object | Assignment Description
---|---
Organizational Units | Assign a policy to OUs to have the policy apply to users and computers belonging to the OU.
Groups | Assign a policy to User or Computer groups that were already defined in the active directory.
  
If you assign a policy to an Active Directory group, a node may belong to more than one group, and therefore it will enforce the policy of the highest ranking group to which it belongs.
IP Network Range | Use this group to enforce security according to the location of the endpoint, regardless of placement in the active directory. For example, you can use IP Network Ranges to create different policies for users when connecting through your VPN.
  
**Note:** If your organization and endpoints will use a VPN, assign a policy to the Security Gateway to ensure that users have the appropriate access.
Individual endpoint users | Assign a policy directly to one or more users to provide exceptions to your general security practices.
Individual endpoint computers | Assign a policy directly to one or more computers to provide exceptions to your general security practices.

### Viewing Assignments

After you create a policy configuration, you can see the assignments of nodes.

**To view policy assignments:**

1. On the Policies tab, select a blade. The **Overview** page for that blade shows
2. In the **View by** box, select **Assignment**. The console shows each node that has this policy
3. Click **Overview** in the tree.
4. The **Policy Overview** page shows:
   - **Policy Assignment per blade**, a way of seeing how many policies are in use
   - **Policy Status**, which policies are installed and when.

### Deploying Policies

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

To install a policy on assigned nodes, on the **File** menu, click **Install Policies**. Or by clicking the **Install Policies** button.

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

### Managing Users

Manage individual users from the **User Details** window. This window shows a user's details and assigned policies. You can configure a user's Preboot authentication method and password.

You can edit a policy from the **User Details** window. All changes apply everywhere that policy is installed. To change the policy of specified users only, you must create a customized policy for them.
From the User Details window you can use these options:

- **General Details** - See the computer assigned to the user, its status and the status of each blade on the computer. If the user has multiple computers, select one to see its status.
- **Policy Assignments** - See all policies assigned to the user.
- **Security Blades** - Select a blade to see the status of that blade on the user's computer.
- **Security Blades > OneCheck User Settings** - Change a user's Preboot authentication method.

To open the User Details window, double click a user object wherever it is shown in the Endpoint Security Management Console. This procedure is one example of how to open the User Details.

**To open User Details from My Organization:**
1. In the Endpoint Security Management Console, open My Organization.
2. Double-click a folder from the navigation tree to see the users and computers that it contains.
3. Right-click a user and select Edit.
   
The User Details window opens.

### Changing a User's Password

If the Full Disk Encryption blade is enabled on a computer, the user must enter authentication credentials to log in during the Preboot authentication. Change the Preboot authentication method for individual users in the OneCheck User Settings page.

Users can change their own passwords from the Preboot. You can manage user Preboot passwords from the User Details window.

**To change a user's Preboot password from the Endpoint Security Management Console:**
1. In the User Details > Security Blades > OneCheck User Settings in the Preboot 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 OUs or Groups

Right-click on a node in the My Organization tree and click Edit to see details for the group or OU.

You can edit a policy from the OU Details or Group Details window. All changes apply everywhere that policy is installed. To change the policy of specified groups only, you must create a customized policy for them.

From the OU Details or Group Details window you can use these options:

- **General Details** - See a summary of the status of the computers in the OU and the blades and policies installed.
- **Content** - See the users and computers that are included in the OU.
- **Policy Assignments** - See all policies assigned to the OU.
- **Security Blades** - Select a blade to see the status of that blade on computers in the OU.
- **Security Blades > OneCheck User Settings** - Add and remove administrators who are authorized to log on to all computers in the group.

### Disabling the Preboot Temporarily

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

You enable and disable Temporary Preboot Bypass for a computer, group, or OU from the computer or group object in the Endpoint Security Management Console. The Preboot settings in the Full Disk Encryption policy set how Temporary Preboot Bypass behaves when you enable it for a computer.
Temporary Preboot 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 Preboot Bypass turns off automatically and Preboot protection is enabled again.

If you temporarily disable Preboot for a group, the setting is for computers that are part of that group at the time when you save the changes. If you add a computer to the group, manually change the setting on the computer object itself.

**To temporarily disable Preboot 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 **Disable Preboot Protection**.
2. Click **Temporarily Disable Preboot**.
3. Click **Yes**.

The Preboot is enabled again when you click **Revert to Policy Configuration** or when the criteria in the Temporary Preboot Bypass settings ("Temporary Preboot Bypass" on page 92) are met.

---

**Managing Computers**

Manage individual computers from the **Computer Details** window. This window shows computer details and the policies and user assigned to them. You can configure which users can log on the computer.

You can edit a policy from the Computer Details window. All changes will apply everywhere that policy is installed. To change the policy of specified computers only, you must create a customized policy for them.

From the **Computer Details** window you can use these options:

- **General Details** - See the users assigned to the Computer, their status and the status of each blade on the computer.
- **Policy Assignments** - See all policies assigned to the computer or the computer's user.
- **Security Blades** - Select a blade to see the status of that blade on the computer.
- **Security Blades > OneCheck User Settings** - Change the users who can authenticate to the computer during Preboot.
- **Security Blades > Full Disk Encryption** - Temporarily disable Preboot.

To open the **Computer Detail** window, double-click a Computer object wherever it is shown in the Endpoint Security Management Console. This procedure is one example of how to open **Computer Details**.

**To open the Computer Details from My Organization:**

1. In the **Endpoint Security Management Console**, open **My Organization**.
2. Double-click a folder from the navigation tree to see the computers (Machine) and users that it contains.
3. Right-click a Machine and select **Edit**.
   
   The **Computer Details** window opens.

---

**Managing Users of a Computer**

If the Full Disk Encryption blade is part of an Endpoint Security client's policy, only users that are configured for a specified computer can log on to that computer.

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

**To add users to a computer:**

1. Right-click a Computer object and select **Computer Details > Security Blades > OneCheck User Settings**.
   Or, right-click a Computer object and select **Authorize Preboot users**.
2. In the **Authorized Preboot Users** area, click **Add**.
3. In the window that opens enter a User or Logon Name or browse to find one.
4. Click **OK**.
5. Click **OK**.
6. Select **File > Save**.
To remove a user from the computer:
2. In the Authorize Preboot Users area, select a user from the list shown.
3. Click Remove.
4. Click Yes.
5. Click OK.

Resetting a Computer

When the Endpoint Security client is installed on a computer, information about the computer is sent to and stored in the Endpoint Security Management server. If you reset a computer object, this information is deleted from the Endpoint Security Management server.

**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.

If these conditions exist, you might choose to reset a computer:
- 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.

When you reset a computer, it:
- 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 Preboot settings.
- Is marked as unregistered

Resetting a computer does not change its position in the My Organization structure.

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 My Organization tab or anywhere in the Endpoint Security Management Console where a computer object is shown, right-click a computer and select Reset Computer.
2. When the Reset Computer message opens, click Yes.
3. Select File > Save.
Chapter 8

Management High Availability

In This Chapter

Overview of High Availability in Endpoint Security 70
The High Availability Environment 70
High Availability Deployment Considerations 71
Active versus Standby 71
Changing a Server to Active or Standby 71
Synchronizing the Active and Standby Endpoint Security Management Servers 72
Understanding the Status of the High Availability Environment 74
Updating the PAT Version on the Server 74

Overview of High Availability in Endpoint Security

The Endpoint Security Management server consists of multiple databases with data on different aspects of the system, such as network objects, users, and policy information. When the administrator makes modifications to the system, this data is updated. Management High Availability lets you create one or more backup Security Management Servers. Each Security Management Server contains a backup Endpoint Security Management server to:

- Have a secure, synchronized backup of this all data.
- Have a backup server to replace the Endpoint Security Management server during down time.

In Management High Availability, the Active Endpoint Security Management server (Active ESM) always has one or more backup Standby Endpoint Security Management server (Standby ESM) which is prepared to replace the Active Security Management server. These Endpoint Security Management servers must all be of the same Operating System and version. You can use different versions of Windows Operating Systems with each other. The Endpoint Security Management servers synchronize regularly.

For initial installation and configuration procedures, see Installing a Server for High Availability (on page 21).

The High Availability Environment

The Management High Availability environment requires an Active ESM and at least one Standby ESM.

When you install the first Endpoint Security Management server, you configure it as the Primary Security Management server. This is the regular Endpoint Security Management server used to manage the Endpoint Security environment. When you install more Endpoint Security Management servers, configure them as Secondary Security Management servers.

The Secondary Security Management server is created with empty databases. These databases will be filled with information from the Primary Security Management server. The Secondary Security Management server is ready after:

- It is represented on the Primary Security Management server by a network object.
- SIC trust is created between it and the Primary Security Management server.
• It has synchronized with the Primary Security Management server for the first time. You must do this manually.

When the Secondary Security Management server is ready, the distinctions between Primary and Secondary are no longer important. These servers are called Active or Standby, according to their role in the Management High Availability environment. Each Endpoint Security Management server can be the Active ESM.

High Availability Deployment Considerations

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

- **Remote versus Local Installation of the Standby ESM** - It is good to install a Standby ESM remotely and not on the LAN. If there are connectivity issues on the LAN the remote Standby ESM will not be affected.

- **Different physical locations** - It is good to have at least one Standby ESM in a different location than the Active ESM to keep 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 Endpoint Security Management servers is quick and efficient.

Active versus Standby

The Active ESM does all management operations, such as editing and installing the Security Policy and modifying users and objects. Security Gateways and Endpoint Clients fetch the Security Policy from the Active ESM.

If the Standby ESM must replace the Active ESM, you must make changes in the correct sequence to prevent data loss:

- If the Active ESM is responsive:
  a) Manually synchronize the Active and Standby ESMs.
  b) Manually change the Active ESM to Standby.
  c) Manually change the Standby ESM to Active.
  d) Make sure that the PAT versions on the Active and Standby ESMs are the same ("Updating the PAT Version on the Server" on page 74).

- If the Active ESM is down and you cannot change it:
  a) Manually change the Standby ESM to Active.
  b) Edit the PAT version on the new Active ESM ("Updating the PAT Version on the Server" on page 74).

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

Changing a Server to Active or Standby

Whenever possible, change the Active ESM to Standby before you change the Standby ESM to Active.

**To change an Active ESM to Standby:**
1. Connect to the Active ESM 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 ESM to Active:**
1. Connect to the Standby ESM 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.

---

**Synchronizing the Active and Standby Endpoint Security Management Servers**

After the Endpoint Security Management servers are installed, you must start the first synchronization manually. The procedure for the first synchronization is in the Secondary Server configuration instructions ("Secondary Server Configuration in the Console" on page 21).

After the first synchronization, you set the frequency of the synchronization between the Standby ESM and the Active ESM. You can configure the synchronization to occur automatically, or manually. If you choose automatic synchronization, configure which events start the synchronization.

**Note** - While the synchronization takes place, the SmartDashboard shows Not Responding.

**To configure how Synchronization occurs:**
1. 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 ESMs automatically synchronize each time the Policy is installed in the Endpoint Security Management Console or SmartDashboard.
     
     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 when the administrator saves the Security Policy or Endpoint Security policy.
     - **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 ESMs.
3. Click **OK**.
4. Select **File > Save**.

If automatic synchronization is selected as the synchronization mode, you can still synchronize manually.

**To synchronize the Endpoint Security Management servers manually:**
1. In SmartDashboard of the Active ESM, select **Policy > Management High Availability**.
2. Click **Synchronize**.
3. Click **OK**.
4. Select **File > Save**.
5. Manually copy MSI client packages to the Standby servers.
   
   a) On the Active ESM, copy `%fwdir%\conf\SMC_Files\uepm\MSI`.
   
   b) On the Standby ESM, replace the `%fwdir%\conf\SMC_Files\uepm\MSI` file with the file from the Active server.
What Data is Synchronized?

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

- The latest Endpoint Policies all data on the Endpoint Security Management server such as:
  - Object and user databases
  - Software Deployment information.
- Configuration and ICA data, such as:
  - 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.

Important - MSI files are NOT synchronized. Manually copy MSI client packages to the Standby servers.

Synchronization Status

The synchronization status shows the status of the peer Endpoint Security Management servers in relation to the selected Endpoint Security Management servers. You can see this status if you are connected to the Active ESM or a Standby ESM. 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 - Immediately after the Secondary Security Management server is installed, it has not had the first manual synchronization that brings it up to date with the Primary Security Management server.
- Synchronized - The peer is synchronized correctly and has the same database information and installed Security Policy.
- Lagging - Changes were made to the Active ESM after the last synchronization. This is sometimes the status immediately after synchronization because changes can be made to the database during the Synchronization process.
- Advanced - The peer ESM is more up-to-date.
- Database has been changed - This is sometimes the status immediately after synchronization because changes can be made to the database while the synchronization occurs.
- Collision - The Active ESM and its peer have different installed policies and databases.
  You must do a manual synchronization and choose which of the ESMs to overwrite. Start the manual synchronization on the Endpoint Security Management server that has more changes. At this point the system administrator must choose which of the Endpoint Security Management servers will become the Standby ESM, and change its status, if necessary. It might also be necessary to update the PAT Version on the Endpoint Security Management server.

Use Audit Logs to see and monitor management operations and Synchronization operations in SmartView Tracker.

When Synchronization Fails

The synchronization can fail in these situations:

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

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

To see the status of the Endpoint Security Management servers in your High Availability environment:

1. In the SmartDashboard of an Endpoint Security Management server, select **Policy > Management High Availability**.
2. In the localhost window that opens, see the status of the Endpoint Security Management server you are on in **My Status**.
3. See the status of other Endpoint 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 Endpoint 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 Endpoint Security Management servers. See Synchronization Status (on page 73) for complete descriptions.</td>
</tr>
</tbody>
</table>

Updating the PAT Version on the Server

When you change a Standby ESM to Active, the new Active ESM can have an older Policy Assignment Table (PAT) version than the clients. If you cannot synchronize the ESMs before you change a Standby ESM 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 repair this, update the PAT number on the Active server.

**To get the PAT version:**

If the Active ESM is available, get the last PAT version from the current Active ESM.
1. Change directory to %uepmdir%\bin>
2. Run:
   %uepmdir%\bin\uepm patver get

If the Active ESM is not available, get the last PAT version from a client that was connected to the server before it went down.

1. Open the Windows registry.
2. Find HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\EndPoint Security\Device Agent
3. Double-click the PATVersion value.
   The Edit String window opens.
4. Copy the number in the Value data field. This is the PAT version number.

**To change the PAT version on the server:**

1. Open a command prompt.
2. Change directory to %uepmdir%\bin>
3. Run the Endpoint Security Management Security utility (uepm.exe) and set the new PAT version:
   %uepmdir%\bin\uepm patver set <new_PAT_version_number>
4. Make sure the new PAT version is set by running:
   %uepmdir%\bin\uepm patver get
Chapter 9

External Endpoint Policy Servers

In This Chapter

Overview of Endpoint Policy Servers 76
How do Endpoint Policy Servers Work? 76
Configuring Policy Server Settings 77
Monitoring Endpoint Policy Server Activity 79

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.

We recommend that you use a distributed deployment of external Endpoint Policy Servers on dedicated machines. This includes:

- At least one Endpoint Policy Server for each remote site.
- In larger sites, multiple Endpoint Policy Servers to improve performance.

For installation and initial configuration instructions, see Installing External Endpoint Policy Servers (on page 19).

How do Endpoint Policy Servers Work?

The Endpoint Policy Servers sit 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. The Endpoint Policy Servers manage:

- All heartbeat and synchronization requests.
- All messages about Blades. For example, messages related to Full Disk Encryption or Media Encryption.
- Other system messages.
- All client logs.

The Endpoint Policy Servers collect this information and send it to the Endpoint Security Management server.

If there are multiple Endpoint Policy Servers in an environment, each client does an analysis to find which Endpoint Policy Server is closest and automatically communicates with that server.
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 Policy servers on the list. The server that replies the fastest is considered to be closest.

The server list is an XML file called `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:

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 policy server replies before the New York 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 the Proximity Analysis Interval

To change the interval after which the clients do an analysis to find the closest Endpoint Policy Server:

1. In the Endpoint Security Management Console, select **Manage > General Properties > Connection Settings**.
2. Set the interval next to **Client will re-evaluate the nearest Policy Server after**. The default interval is 120 minutes.
3. Click **OK**.
4. Select **File > Install Policies** or click the **Install Policies** icon.

Enabling the Management Server to be a 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 the Endpoint Security Management Console, select Manage > General Properties > Connection Settings.
2. Clear Enable Endpoint Management Server to be Endpoint Policy Server.
3. Click OK.
4. Select File > Install Policies or click the Install Policies icon.

**Policy Server and Management Server Communication**

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

- **Endpoint Policy Servers get from the Endpoint Security Management server:**
  - Policies and installation packages.
  - All files that it needs for synchronization.
- **Endpoint Policy Servers send a heartbeat message to the Endpoint Security Management server at 60 second intervals.**
  
  You can change this in the `%uepmdir%\engine\conf\global.properties` file on the Endpoint Security Management server. The property name is `connectionpoint.hb.interval.secs`.
- **Endpoint Policy Servers send sync messages to the Endpoint Security Management server when synchronization is necessary.**
  
  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 Monitoring 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 the Endpoint Security Management Console, 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 Monitoring 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 Monitoring tab.

**Configuring Log Forwarding**

By default, Endpoint Policy Servers are defined as Log Servers. Logs from the client are reported to the Policy Server that the client is connected to.

To view all collected logs together in SmartView Tracker, you must configure Log Forwarding for each Endpoint Policy Server in the SmartDashboard.
To configure Log Forwarding from a Endpoint Policy Server to the Endpoint Security Management server:
1. Open SmartDashboard and connect to the Endpoint Security Management Server.
2. Double-click the Endpoint Policy 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 Endpoint Security Management server.
5. Click OK.
6. Select Policy > Install Database and install the database on all hosts.
Repeat this procedure for each Endpoint Policy Server.

Monitoring Endpoint Policy Server Activity

You can see the status of Endpoint Policy Servers in the Monitoring tab of the Endpoint Security Management Console.

In the Monitoring 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 the Endpoint Security Management Console.
  - IP Address - The IP Address entered for the server.
  - DN - Its full DN name, taken from SmartDashboard.
  - Active - If the server is Active or Not Active. Active means that the server recently sent a heartbeat message.
  - Last Contact - When the Endpoint Security Management server last received a heartbeat message from it.
  - Comments - Comments written for that server in Properties window.

For more detailed information, you can look at the log messages on the Endpoint Policy Server. They are in:
%uepmdir%\logs

You can see if there are errors in the logs and resolve them if necessary.
Chapter 10
Backup and Restore

In This Chapter

Overview of Backup and Restore 80
Prerequisites 80
How to Back Up and Restore 80
Updating the PAT Version on the Server after Restore 81

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 host name as the source server.
- The source and the target servers are primary Endpoint Security servers. The export and import operations are not supported from or to a secondary server.

How to Back Up and Restore

To Back up Endpoint Security data:
1. Open a command prompt on the source server.
2. Change directory to: %FWDIR%\bin\upgrade_tools
3. Run Migrate.exe export with the full path to the output (.tgz) file.
   For example: %FWDIR%\bin\upgrade_tools> migrate.exe export <output_file_name>
The utility generates the .tgz file in the %FWDIR%\bin\upgrade_tools directory.

To restore Endpoint Security data:
1. Copy the .tgz file from the source server to the target server.
2. Open a command prompt.
3. Change directory to: %FWDIR%\bin\upgrade_tools
4. Run Migrate.exe import with the full path to the input (.tgz) file.
   For example: %FWDIR%\bin\upgrade_tools> migrate.exe import <input_file_name>
   The migrate utility:
   • Extracts the configuration files from the .tgz.
   • Copies them to the correct places.
   • Restores the Endpoint Security management and Security Management Server databases.
5. When prompted, restart the target server.

Updating the PAT Version on the Server after Restore

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

To get the PAT version from a client connected to the server:
1. Open the Windows registry.
2. Find HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\EndPoint Security\Device Agent
3. Double-click the PATVersion value.
   The Edit String window opens.
4. Copy the number in the Value data field. This is the PAT version number.

To change the PAT version on the server:
1. Open a command prompt.
2. Change directory to $uepmdir$%\bin$>
3. Run the Endpoint Security Management Security utility (uepm.exe) and set the new PAT version:
   $uepmdir%\bin>uepm patver set <new_PAT_version_number>
4. Make sure the new PAT version is set by running:
   $uepmdir%\bin>uepm patver get
Chapter 11

OneCheck User Settings Policies

You can define policies and assign them to different networks, directories, and groups in the organization to maximize endpoint client security.

OneCheck User Settings include:

- How users authenticate to Endpoint Security.
- If users can access Windows after they are authenticated to Endpoint Security or if they must also log on to Windows.
- What happens when a user enters invalid authentication details.
- A limit for how many times a user can access a computer.
- If Remote Help is permitted. This lets users get help from an administrator, for example if their computers become locked after too many failed authentication attempts.

Configure the OneCheck User Settings setting in the Policies tab > OneCheck User Settings. Edit a policy there or create a New policy to configure the settings.

Many of these settings relate to the Preboot authentication, which is part of Full Disk Encryption. Make sure to configure the settings for the Full Disk Encryption Policy also in Policies tab > Full Disk Encryption.

In This Chapter

Quick Start 82
Seeing OneCheck User Settings Policy Assignments 83
OneCheck User Settings Assignments 83
Configuring OneCheck User Settings 83

Quick Start

To start with OneCheck Logon policies, you can use the predefined policies.

- **High Security OneCheck User Settings Logon** - Default high security policy.
- **Medium Security OneCheck User Settings Logon** - Default medium security policy.

To assign a predefined policy:

   The OneCheck User Settings Overview page opens.
2. Double-click one of the predefined policies.
   The OneCheck User Settings Policy window opens.
3. Review the settings in the Policy. Use this Administration Guide to understand the settings. If you are satisfied with the predefined settings, continue with the next step. If you are not satisfied, create a new policy.
4. Click Assignment.
5. On the Assignment window, click Add Assignment and select from the Navigation tree. Click OK.
   The assignment is shown in the Assignment window.
6. Click OK.
Seeing OneCheck User Settings Policy Assignments

You can see all OneCheck User Settings Policies assignments. Policies can be attached to the entire organization, directories, groups, users, and endpoint computers. Multiple policies can be assigned.

To show policy assignments:
1. On the OneCheck User Settings Overview page, click the View By list
2. Select Assignments.

OneCheck User Settings Assignments

To assign a policy:
1. In the Policies tab, in the Overview page of a blade, open an existing policy or create a new one.
2. The Policy window opens.
3. Click Assignment in the navigation tree.
4. Click Add Assignment.
   The Select Node window opens.
5. In the Navigation Tree, select a node in the directory. When you select a directory or group, users that belong to that group or directory show in the Node area.
6. Click OK.
7. On the Assignment page, click the Add Assignment down arrow, and select from the displayed options.
8. Click OK.
9. Click Install Policies.

To assign a different policy:
1. On the Assignment page, select the node row and click the Assign Different Policy down arrow.
   The list of policies is shown.
2. Select a policy.
3. Click OK.
4. Click OK.
5. Click Install Policies.

Configuring OneCheck User Settings

There are many settings that you can configure for OneCheck User Settings.

To configure OneCheck User Settings:
1. Click the Policies tab > OneCheck User Settings.
2. In the View by drop-down list, select Policies.
3. To edit an existing OneCheck User Settings configuration, select one in the list and click Edit.
   To define a new OneCheck User Settings configuration, click New.
4. Configure the settings in the different categories of the OneCheck User Settings window.

Account Lockout

These settings determine the lockout behavior when the user exceeds the assigned number of failed logons.
### Configuring OneCheck User Settings

#### Policies

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of failed logons before account is locked</td>
<td>The maximum number of failed logon attempts allowed before the user account is locked. If the account becomes locked, the user will no longer be allowed to log on to the computer. To remedy the situation, the user will have to receive Remote Help from an administrator.</td>
</tr>
<tr>
<td>Number of failed attempts before a temporary lockout</td>
<td>The maximum number of failed logon attempts allowed before the user account is temporarily locked out from the computer for a defined duration.</td>
</tr>
<tr>
<td>Duration of a temporary lockout</td>
<td>If the temporary lockout option is selected, this sets the duration of a temporary lockout, in number of minutes.</td>
</tr>
<tr>
<td>Maximum number of successful logons allowed before the account is locked</td>
<td>The maximum number of times that a user can log on to Endpoint Security. When this is reached, the user account cannot be used. To unlock an account, you must disable this feature in the active policy or increase this value for the policy. Remote Help cannot be used.</td>
</tr>
</tbody>
</table>

#### Password Security

Use these settings to set required security parameters for passwords.

If you use password synchronization, we recommend that users' Windows password and Preboot password have the same requirements. This prevents problems with the first Preboot logon, OneCheck Logon, and Single Sign-On.

Expand the **Advanced** category in the OneCheck User Settings window to see the Password Security options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Level</td>
<td>Disable Windows' password security configurations and set your own password requirements.</td>
</tr>
<tr>
<td>Default Level</td>
<td>Enforces password requirements similar to the Windows complexity requirements. 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 three of these categories: uppercase, lowercase, numeric characters, symbols.</td>
</tr>
<tr>
<td></td>
<td>- Not have the user name or full name.</td>
</tr>
</tbody>
</table>

**Password Security - Custom Level**

To set your own options for password security (rather than choosing a predefined security level), click **Custom Level**. A new window opens, displaying these options:

- **Note** - You can see the requirements for each security level on the screen when you click **Default** and move the slider between the different options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Windows complexity requirements</td>
<td>This setting ensures that the standard Windows password requirements are enforced.</td>
</tr>
<tr>
<td></td>
<td>The password must:</td>
</tr>
<tr>
<td></td>
<td>- Have at least six characters</td>
</tr>
<tr>
<td></td>
<td>- Have characters from at least 3 of these categories: uppercase, lowercase, numeric characters, symbols.</td>
</tr>
</tbody>
</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.

Minimum length of password | Enter the minimum number of characters for a valid password.

Password can be changed only after | Enter the minimum number of days that a password must be valid before the user can change it.

Password expires after | Enter the maximum number of days that a password can be valid before the user must change it.

Number of passwords | Enter the minimum number of password changes needed before a previously used password can be used again.

### OneCheck User Settings Permissions

OneCheck User Settings Permissions define when the user can access the computer and if the user can get Remote Help. Expand the Advanced category in the OneCheck User Settings window to access the Permissions category.

<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 preboot to a system in hibernate mode.</td>
</tr>
<tr>
<td>Allow user of recovery media</td>
<td>Let user authenticate to use recovery media to recover and decrypt data from an encrypted system. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Allow user to change his credentials from the endpoint client</td>
<td>Let users change the password on an endpoint client during the Preboot.</td>
</tr>
<tr>
<td>Allow Single Sign-On use</td>
<td>Let users use Single Sign On to log on to Preboot and Windows when OneCheck Logon is disabled. Single Sign on applies only to Preboot 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 can give 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.

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.

- **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 use Remote Help:

**Important** - Users can only use Remote Help if Remote Help is also enabled for the computer in Full Disk Encryption policy > General Properties > Preboot Protection > Configure > Enable Remote Help. It is enabled by default in the predefined policies. Make sure it is enabled in all Custom settings.

Make sure these options are selected in **OneCheck User Settings > Advanced > Permissions**.

### Remote Help Permissions Settings

<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>
Full Disk Encryption Policies

Check Point Full Disk Encryption gives you the highest level of data security. It combines boot protection with Preboot 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 are automatically fully encrypted. This includes system files, temp 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.

- **Preboot Protection** - Users must authenticate to their computers in the Preboot, 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 the Endpoint Security Management Console in the Policies tab > Full Disk Encryption. Edit a policy there or create a New policy to configure the settings.

Make sure to configure the OneCheck User Settings Policy also in the Policies tab > OneCheck User Settings. Edit a policy there or create a New policy to configure the settings. Many of the settings that relate to the Preboot are configured there.

Quick Start

This section explains how to quickly assign predefined Full Disk Encryption policies.

**To Quickly Assign a Predefined Policy:**

1. In the Endpoint Security Management Console, open the Policies tab.
2. Select Full Disk Encryption from the Navigation tree.
   
   The Full Disk Encryption Overview page shows two built-in policies:
   
   - Medium Security Full Disk Encryption Policy
   - High Security Full Disk Encryption Policy
3. Double-click one of the predefined policies.
   
   The Full Disk Encryption Policy window opens.
4. Review the settings in the Policy. Use this Administration Guide to understand the settings. If you are satisfied with the predefined settings, continue with the next step. If you are not satisfied, create a new policy.
5. Click Assignment.
6. On the Assignment page, click the downward-facing arrow on the Add Assignment button.
7. Click Connected to Enterprise.
8. The Select Node window opens.
9. Select a node in the Active Directory.
10. Click OK.
   The Select Node window closes, and the new assignment is shown on the Assignment page.
11. Click OK.

Seeing Full Disk Encryption Policy Assignments

You can attach one or more Policies to the whole organization, or directories, groups, users and endpoint computers in it.

To show policy assignments:
1. On the Full Disk Encryption Overview page, click the View By list
2. Select Assignments.

Creating a Customized Full Disk Encryption Policy

Create customized Policies applicable to your network.

To Create a Customized Policy:
   The Full Disk Encryption Policy Overview page shows.
2. From the View By drop-down box, select Policies.
3. Click New:
   The Full Disk Encryption Policy window opens.
4. On the General Properties page, configure Full Disk Encryption settings for:
   - Drive Encryption (on page 88)
   - Preboot Protection
   - User Acquisition (on page 93)
   - OneCheck
5. Click Assignment.
   The Assignment page opens. Assign the policy to all of the organization, directories, groups, users, or endpoint computers.
6. Click OK.

Drive Encryption

You can use the slider to set the encryption level or configure the settings individually.
Creating a Customized Full Disk Encryption Policy

Security Level | Meaning
---|---
Custom | - Newly added drives are not encrypted
- By default, volumes are encrypted using AES
- IRRT devices are not encrypted
- Custom drive and volume encryption settings let you specify drives, volumes, and whether they should be encrypted.
- At least one drive must have Preboot protection

Low | - Newly detected drives are not encrypted
- By default, volumes are encrypted using AES
- Minimum encryption for Preboot protection
- Drives and volumes are not encrypted

Medium | - Newly detected drives are not encrypted
- By default, volumes are encrypted using AES
- All existing drives and volumes are encrypted

High | - Newly detected drives are encrypted
- By default, volumes are encrypted using AES
- All existing drives and volumes are encrypted
- Boot protect and encrypt hidden disk volumes

Each level can also be customized by clicking Configure. If you customize any of the levels that then that level becomes the new Custom level. The slider moves to the Custom level position.

Full Disk Encryption can use these encryption algorithms:

- AES (256-bit)
- Blowfish (256-bit)
- Cast (128-bit)
- 3DES (168-bit)

Preboot Protection

Preboot is a program that prevents the Windows operating system from booting until the user authenticates.

You can synchronize:

- The Preboot Windows and Network login values by configuring OneCheck User Settings properties.
- The Preboot Windows login by configuring Single Sign On properties, which uses the Microsoft Windows Strong Authentication Protocol.

To configure the settings for Preboot Protection:

1. On the General Properties page of the Full Disk Encryption Policies window, you can use the slider to select one of the predefined settings. We recommend that you click Configure to select the exact settings for Preboot Bypass and Temporary Preboot Bypass based on your environment.

Security Level | Meaning
---|---
Custom | - Preboot Protection is disabled
- Temporary Preboot Bypass is disabled after three failed logon attempts or 3 days
- Preboot is enabled after 9 failed logon attempts to Windows
- Remote Help enabled
- Hardware Hash enabled

Note: These default settings can be adjusted.
Creating a Customized Full Disk Encryption Policy

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low User Trust</td>
<td>• Preboot Protection is disabled</td>
</tr>
<tr>
<td></td>
<td>• Temporary Preboot Bypass is disabled after three failed logon attempts or 3 days</td>
</tr>
<tr>
<td></td>
<td>• Preboot is enabled after 9 failed logon attempts to Windows</td>
</tr>
<tr>
<td></td>
<td>• Remote Help enabled</td>
</tr>
<tr>
<td></td>
<td>• Hardware Hash enabled</td>
</tr>
<tr>
<td>Medium User Trust</td>
<td>• Preboot is enabled</td>
</tr>
<tr>
<td></td>
<td>• Temporary Preboot Bypass is disabled after 2 logon attempts or 2 days</td>
</tr>
<tr>
<td></td>
<td>• Remote Help enabled</td>
</tr>
<tr>
<td>Higher User Trust</td>
<td>• Preboot is enabled</td>
</tr>
<tr>
<td></td>
<td>• Temporary Preboot Bypass is disabled after 1 automatic logon or 1 day</td>
</tr>
<tr>
<td></td>
<td>• Remote Help enabled</td>
</tr>
</tbody>
</table>

2. Click **Advanced** to set these Preboot Environment Permissions:

   **Note** - These permissions are also in the Preboot Customization Menu on client computers. To open the Preboot Customization Menu, press both shift keys on a client computer while Full Disk Encryption loads during the start up.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable USB device in preboot environment</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 Preboot.</td>
</tr>
<tr>
<td>Enable PCMCIA</td>
<td>Enables the PCMCIA Smart Card reader. If you use Smart Cards that require this, make sure it is enabled.</td>
</tr>
<tr>
<td>Enable mouse in preboot environment</td>
<td>Lets you use a mouse in the Preboot environment.</td>
</tr>
<tr>
<td>Allow Serial Over LAN in preboot environment</td>
<td>Lets administrators log onto the Preboot environment remotely with an Intel vPro-enabled PC and a telnet session to the client.</td>
</tr>
<tr>
<td>Allow low graphics mode in preboot environment</td>
<td>Select to display the Preboot 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.                                                                                                                                                                                                                           |
Note - Users assigned to a higher level node in the AD who have permission to log into a preboot environment can also log into the Preboot environments of computers below them in the AD hierarchy. However, in the Endpoint Security Management Console, the higher level user is not shown under **Allowed Users To Logon** for the lower level computer.

3. Click **Configure** for more granular control over:
   - Preboot Bypass (on page 91)
   - Temporary Preboot Bypass (on page 92)
   - Remote Help (on page 93)

**Preboot Bypass**

Preboot Bypass disables Preboot protection and users go straight to the Windows login. It was previously called Windows Integrated Login (WIL). Check Point does not recommend that you use this option.

Preboot Bypass makes the user experience simpler when users log on to encrypted drives, but it also limits the strength of the computer's security configuration. As an alternative to Preboot Bypass, consider Single Sign-On (SSO) in conjunction with proper Preboot Authentication.

**To configure Preboot Bypass:**
1. On the **General Properties** page of the Full Disk Encryption Policies window > **Preboot Protection** area, click **Configure**.
2. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Preboot Bypass</td>
<td>Select this to enable Preboot Bypass.</td>
</tr>
<tr>
<td>Maximum failed logons in Windows before Preboot Bypass is disabled</td>
<td>If the number of failed logon attempts exceeds the number of tries specified, Preboot Bypass is disabled. The computer automatically reboots and the user must authenticate in Preboot. If the Maximum Failed Logon value is set to 1 and the end-user logs on incorrectly, Preboot Bypass is not disabled because the number of logon failures has not exceeded the number entered in this property. However, if the subsequent attempt to log onto Windows fails, Preboot Bypass is disabled.</td>
</tr>
<tr>
<td>Enable Hardware Hash</td>
<td>If selected, the client generates a hardware hash from identification data found in the BIOS and on the CPU. If the hard drive is stolen and put in a different computer, the hash will be incorrect and Preboot Bypass will be disabled. The computer reboots automatically, and the user must authenticate in Preboot. <strong>Warning:</strong> Disable Preboot Bypass before upgrading BIOS firmware or replacing hardware. After the upgrade, the hardware hash is automatically updated to match the new configuration.</td>
</tr>
<tr>
<td>Bypass failure Preboot message</td>
<td>Enter a message to display to the user if Preboot Bypass fails. For example, to call the Help Desk if the Preboot window opens.</td>
</tr>
</tbody>
</table>
Enable location awareness according to network locations

To make sure that the client is connected to the correct network, the computer pings a defined number of IP addresses during the boot process.

If none of the IP addresses replies in a timely manner, the computer might have been removed from the trusted network and Preboot Bypass is disabled. The computer reboots automatically and the user must authenticate in Preboot. If one IP address replies, Preboot Bypass remains enabled.

**Note:** While this option is enabled, Windows cannot be started in Safe Mode.

---

**Temporary Preboot Bypass**

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

You enable and disable Temporary Preboot Bypass for a computer, group, or OU from the computer or group object in the Endpoint Security Management Console. The Preboot settings in the Full Disk Encryption policy set how Temporary Preboot Bypass behaves when you enable it for a computer.

Temporary Preboot 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 Preboot Bypass turns off automatically and Preboot protection is enabled again.

To temporarily disable Preboot on a computer or OU, see Disabling the Preboot Temporarily (on page 67).

**To configure Temporary Preboot Bypass settings:**

1. On the **General Properties** page of the Full Disk Encryption Policies window > Preboot Protection area, click **Configure**.

2. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Endpoint will disable Temporary Preboot Bypass after (number of automatic logons)</td>
<td>Enter the number of times the Temporary Preboot Bypass functionality can be used. After the number of logons expires, Temporary Preboot Bypass is disabled on the client and the Preboot environment shows.</td>
</tr>
<tr>
<td>The Endpoint will disable Temporary Preboot Bypass after (number of days)</td>
<td>Enter the number of days for which Temporary Preboot Bypass functionality is enabled. After the number of days expires, Temporary Preboot Bypass is disabled on the client and the Preboot environment shows. Select a small number so that you do not lower the security by disabling the Preboot for a long time.</td>
</tr>
<tr>
<td>Automatic logon starts after (number of minutes)</td>
<td>Enter the time delay in minutes. After the delay expires, Temporary Preboot Bypass functionality logs the user into the Windows environment. During the delay, the Preboot Login window shows. The user can manually logs into the windows environment.</td>
</tr>
<tr>
<td>Allow Windows Logon</td>
<td>Lets the user log in to Windows after the Temporary Preboot Bypass logon.</td>
</tr>
</tbody>
</table>

---

**Notes**

- Dynamic events on the client, such as a *Network Location Awareness Verification*, disable Preboot Bypass if the event fails.

- If you lower the security by using Preboot Bypass, use different security precautions to protect the computer. We recommend that you configure:
  - Location Awareness (if your users stay with a specified network)
  - Hardware Hash
  - Maximum failed logons in Windows before Preboot Bypass is disabled
Notes -

- Dynamic events on the client, such as a Network Location Awareness Verification, disable Temporary Preboot Bypass if the event fails.
- Temporary Preboot Bypass can be enabled or disabled from the Endpoint Security Management Server command line:
  Device Details > OneCheck User Settings Preboot Settings > Windows Integrated Logon and Wake on LAN settings.
- If the mouse is moved or a key pushed on the keyboard in the Preboot environment, the Temporary Preboot Bypass functionality is disabled.

Remote Help

Users can be denied access to their Full Disk Encryption protected disks for a number of reasons. For example, they might have entered an incorrect password too many times. Remote Help is designed to assist users in these types of situations. Users call the designated Endpoint Security administrator and follow the Remote Help procedure.

To configure Remote Help:
2. Select Enable Remote Help.
3. Make sure the settings in OneCheck User Settings Permissions are also configured to allow users to get Remote Help.

User Acquisition

Full Disk Encryption acquires users when they log on to Windows on the Endpoint Security client computer. When the Preboot runs for the first time, users authenticate with their Windows credentials that Full Disk Encryption collected. Disk encryption and Preboot do not start until the users are acquired.

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 so that Full Disk Encryption can collect their information.

Before you enable automatic User Acquisition, make sure clients can get device and user policies from the server.

To set User Acquisition Criteria:
1. On the General Properties page of the Full Disk Encryption Policies window, in the User Acquisition area, select: Automatically add <number> users that log into the machine as authorized preboot users.
2. Click Advanced.
   The User Acquisition Settings pane opens.
3. Select Enable Automatic Acquisition of Users logged into the client.
4. Select what has to occur before User Acquisition can be complete:
   * The acquisition process has acquired (x) user(s) - Select the number of users that must log on to the computer during the user acquisition process
     If you enter 3, the user acquisition service is active until 3 users log on to the computer. However, if you also limit the acquisition period to a specific number of days, user acquisition ends if at least one user has been acquired and registered during the time limit.
   * At least one user has been acquired after x day(s) - Select how long to wait to get the configured number of users.
     This limits the number of days when user acquisition is active for the client. If the limit expires and one user is acquired, Full Disk Encryption can be enforced and User Acquisition ends. If no users are acquired, user acquisition from the Active Directory continues.

   **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 user 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
- Media Encryption & Port Protection
- 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.

If you use password synchronization, we recommend that users’ Windows password and Preboot password have the same requirements. This prevents problems with the first Preboot logon, OneCheck Logon, and Single Sign-On.

If you use Single Sign-On, but not OneCheck, the logon applies to Windows and Full Disk Encryption but not different blades.

You can use Smart Cards for preboot authentication with OneCheck Logon or Single Sign-On enabled.

To configure OneCheck Logon:

On the General Properties page of the Full Disk Encryption Policies window:

1. Select Enable OneCheck to replace Windows Authentication Logon Screen.
2. Click Advanced.
   - The OneCheck Logon window opens.
3. Select Enable OneCheck.
4. Optionally 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.
5. Optionally, select Require that only an authorized preboot user is allowed to log into Windows. If selected, only users that have permission to authenticate to the Preboot on that computer can log in to Windows.

Password Synchronization

If you plan to use OneCheck Logon, we recommend that you keep the Windows and Preboot passwords synchronized with the password synchronization feature. This ensures that both passwords are the same, and users can use each one, if necessary.

To keep the Windows and Preboot passwords synchronized:

2. Make sure that these options are selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Windows password to match preboot password</td>
<td>The Windows password changes automatically if the user changes the Endpoint Security password.</td>
</tr>
<tr>
<td>Change preboot password to match Windows password</td>
<td>The Endpoint Security password changes automatically if the user changes the Windows password.</td>
</tr>
</tbody>
</table>

Policy Assignment

To assign a policy:

1. In the Policies tab, in the Overview page of a blade, open an existing policy or create a new one.
2. The Policy window opens.
3. Click Assignment in the navigation tree.
4. Click Add Assignment.
   The Select Node window opens.
5. In the Navigation Tree, select a node in the directory. When you select a directory or group, users that belong to that group or directory show in the Node area.
6. Click OK.
7. On the Assignment page, click the Add Assignment down arrow, and select from the displayed options.
8. Click OK.
9. Click Install Policies.

To assign a different policy:
1. On the Assignment page, select the node row and click the Assign Different Policy down arrow.
   The list of policies is shown.
2. Select a policy.
3. Click OK.
4. Click OK.
5. Click Install Policies.

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 Preboot 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 FDE 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.
- User acquisition must be enabled and 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 Preboot).
- 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 Preboot cannot open.

Client Requirements for Full Disk Encryption Deployment

Clients must have:
- 32MB of continuous free space on the client’s system volume

  Note - During deployment of the Full Disk Encryption blade on the client, the Full Disk Encryption service automatically defragments the volume to create the 32MB of continuous free space, and suspends the Windows hibernation feature while the disk is encrypted.

Clients must not have:
- RAID
- EFI (Extensible Firmware Interface)
• Partitions that are part of stripe or volume sets
• On Windows XP, the root directory cannot be compressed. Subdirectories of the root directory can be compressed.

**Completing Full Disk Encryption Deployment on a Client**

Users will have to reboot their computers twice while Full Disk Encryption deploys. One time to make sure the Preboot 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.
- The Endpoint Security Management Console - 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 Preboot. 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 Windows from starting on a client computer, you can use **Full Disk Encryption Recovery Media** to decrypt the computer and recover the data. Client computers regularly send recovery files to the Endpoint Security Management server 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 Windows can run without the Preboot.

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 two 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 Policy > Advanced > Permissions) 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. The media can be on a CD/DVD, USB device, or REC file.

Users who can only authenticate in the Preboot with Smart Cards must use the option shown below to create a temporary user who can use the recovery media.

**Note** - Creating a recovery media on a USB flash disk formats the device and removes all previous content.

**To create recovery media:**
1. In the Endpoint Security Management Console, open My Organization.
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 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: by CD or USB device.

**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** window 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.

**Upgrading Full Disk Encryption**

If you upgrade Endpoint Security from R80 or R80.10, no special actions are required for Full Disk Encryption. Do the procedures in Upgrading Clients (on page 49).

**What effect does an upgrade have on users?**
The upgrade does not have a significant effect on users.

**Upgrading Legacy Full Disk Encryption**

You can upgrade to this Endpoint Security version from Full Disk Encryption Version 7.x or Pointsec PC 6.3.1 HFA 1 and higher. 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 49).
- 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. Make sure that all clients are connected to the server and receive the update.
3. Install a new Initial Client on the legacy client computers.

**What effect does an upgrade have on users?**
- Users are instructed to use their Windows password for the first Preboot after the upgrade and deployment completes.
The Preboot page looks slightly different.

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 Preboot environment on the client.

Run CPinfo if:

- Encrypting or decrypting fails on Windows.
- The selected disk or volume does not encrypt or decrypt.
- Full Disk Encryption related issues occur.
- You experience system issues or crashes.

CPinfo gathers:

- All files in the data directory.
- Installation log.
- File version data for executables.
- Registry values for Full Disk Encryption
- GinaDll, UpperFilters and ProviderOrder.
- SMBios structure.
- Installed application lists.
- Microsoft Windows Partition list.

To Run CPinfo:

1. In the notification area, right-click the client icon.
2. Select Display Overview.
3. In the right pane, click Advanced.
4. Click Collect information for technical support.
   CPinfo opens in the command prompt.
5. Press ENTER to start.
   The information is collected. A window opens that shows the location of the cab file.
6. Press a key to exit CPinfo.

To Run CPinfo manually:

1. Open a command prompt.
2. Go to the CPinfo tool path location: cd \path\.
3. Run CPinfo with output filename and folder:
   C:\\path\\>CPinfo.exe <output cab filename> <output folder name>
   For example: C:\\path\\>CPinfo.exe SR1234 temp.
   The CPinfo application stores the output to the designated folder.

   - If no output name is specified, the output file has the same name as the output folder.
   - If no output folder is specified, CPinfoPreboot saves the output file to the directory where the CPinfo tool is located.
Using CPinfoPreboot

Run CPinfoPreboot if you cannot:

- Access the Preboot Logon window.
- Log in to the Preboot 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 Preboot 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 Preboot 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 cab filename> <output folder name>`. For example: C:\path\CPinfoPreboot.exe SR1234 temp.
4. CPinfoPreboot stores the output file to the designated folder.
   - If no output name is specified, the output file has the same name as the output folder.
   - If no output folder is specified, CPinfoPreboot saves the output file to the working directory on the external media. An output folder is required if the working directory is on read-only media.

Debug Logs

You can use the debug logs to examine the deployment phase or problems that occur. The information there is included in CPinfopreboot. Send the full results of CPinfopreboot to Technical Support for analysis.

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Path to log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\All Users\Application Data\CheckPoint\Endpoint Security\Full Disk Encryption</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>C:\ProgramData\CheckPoint\Endpoint Security\Full Disk Encryption</td>
</tr>
<tr>
<td>Windows 7</td>
<td>C:\ProgramData\CheckPoint\Endpoint Security\Full Disk Encryption</td>
</tr>
</tbody>
</table>

Preboot Issues

Mouse or Keyboard Trouble
If users have trouble with their mice or keyboards during Preboot, you might need to change the setting of Enable USB device in preboot environment. This setting is in the Full Disk Encryption Policy > Preboot Settings. You can also change this setting from the Preboot Customization Menu by pressing both shift keys while Full Disk Encryption is loading when the computer starts up.

Trouble with Password on First Preboot

When the Preboot 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 Preboot, 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.

Full Disk Encryption Logs

Full Disk Encryption utilizes the client logger module for audit logging. Logs are created in the Preboot and Windows environments. Logs created in Preboot 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 FDEInsrtallDLL.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 HELPMMSG 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 Preboot password requirements must not be stricter than the Windows logon password requirements. If the password requirements of Windows and the Preboot do not match, change the password settings for the Preboot password.
3. Make sure that the necessary connections work and that all processes are running. Make sure that:
   - The FDE Credential Manager (PssoCM32) is active on Windows XP: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order.
   - The FDE Credential Provider (PCP) is active on Windows Vista or Windows 7: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PCP\NetworkProvider.
   - The network connection is stable.
   - The Driver Agent is running and has a connection to the server.
   - The Device Auxiliary Framework is running.
Problem: The deployment is stuck at the encryption.

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.

Dynamic Mount Utility
Chapter 13

Media Encryption & Port Protection Policies

Media Encryption & Port Protection Policies prevent unapproved copying of sensitive data by combining device management, content filtering and centralized auditing with robust media encryption. Media Encryption & Port Protection plugs possible leak points and logs data movement to and from plug and play media.

In This Chapter

Media Encryption & Port Protection Terminology 103
Access to Media Encryption & Port Protection Policies 103
Global Settings on the Overview Page 103
General Properties 104
Advanced Media Log 108
Media Encryption & Port Protection User Alerts 109
Media Encryption Sites 109
Converting Legacy Encrypted Devices to Media Encryption 111
Changing the Group Ranking Order 111

Media Encryption & Port Protection Terminology

• Media Owner - The first user to insert the media into an endpoint computer automatically becomes the media owner - This term applies only to users in active directory environments.

• Encrypted Media User - The owner of the encrypted media can be either the user performing the encryption, or another user selected from the active domain.

Access to Media Encryption & Port Protection Policies

To access Media Encryption & Port Protection settings:
1. Click Policies tab > Media Encryption & Port Protection.
2. To edit an existing Media Encryption & Port Protection policy, select a policy and click Edit.
3. To define a new Media Encryption & Port Protection policy, click New.

Global Settings on the Overview Page

The Media Encryption & Port Protection Policy Overview page lets you configure how encrypted drives and volumes are accessed by users when connected to the Endpoint Security Management server.
To set a predefined Global setting:

- Adjust the Encrypted Media Access Rules slider to one of these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom</td>
<td>Custom Access settings for encrypted media. Owners of the encrypted media can read and modify it, although this can be modified. Use the custom setting to configure access for specific users.</td>
</tr>
<tr>
<td>No Automatic Access</td>
<td>No automatic access to encrypted media. Users need to use offline passwords.</td>
</tr>
<tr>
<td>Media Owner Access</td>
<td>Owners of the encrypted media (the user who encrypted the content) can read and modify content. No access to other users.</td>
</tr>
<tr>
<td>Read Only Access</td>
<td>Owners can read and modify the content. All other users have read only access.</td>
</tr>
<tr>
<td>Full Access</td>
<td>All users can read and modify all encrypted content.</td>
</tr>
</tbody>
</table>

To set a custom security level for access to encrypted removable media:

1. In the Encrypted Media Access Rules area, click Configure.
   - The Custom Encrypted Media Access Rules window opens.
2. Click Add.
   - A new online encrypted media access rule is created with default values.
3. Click the (+) button that shows in the Encrypted Media User column to change the value.
4. Click in the Access Allowed column to open a drop-down box showing these access permissions:
   - Full Access
   - Read Only
   - No Automatic Access
   - If a user belongs to multiple rules, the rules at the top of the table get precedence. To change rule precedence, use the Move Up and Move Down buttons.

General Properties

To see General Properties:

1. Open the Policies tab > Media Encryption & Port Protection
2. From the View by drop-down box, select Policies.
3. Select a policy.
4. Click Edit.
   - The policy window opens on the General Properties page showing these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Access to Non-encrypted Devices</td>
<td>Select to set a policy for access to media that are not encrypted. Either set the slider to a predefined policy or click Configure to open the Custom Device Access Settings window and create a new access policy. Click Advanced Settings to configure more granular settings.</td>
</tr>
<tr>
<td>Control Access to Encrypted Removable Media Devices</td>
<td>These settings are managed globally and can be found in the Policies tab &gt; Media Encryption &amp; Port Protection node &gt; Encrypted Media Access section. You can click Configure to change the settings from here also.</td>
</tr>
</tbody>
</table>
Encrypt Removable Media | Configures whether removable media devices are encrypted. Click Advanced Settings to configure more granular control over the process.
---|---
Scan and Authorize Removable Media | Select to scan devices for threats and authorize them for access. Click Advanced Settings to set a custom level.

Creating Rules for Non-Encrypted Devices

Use the Media Encryption & Port Protection Policy to set what users can do with non-encrypted devices.

To create a custom access rule:

1. In the Media Encryption & Port Protection Policy General Properties window, select Control Access to Non-encrypted Removable Media and Peripheral Devices.
2. Move the slider to set the access to not encrypted devices. As you move the slider, the description shows next to it and under it.
3. To configure custom default settings, click Configure. The Custom Device Access Settings window opens.
4. For each device, select what users can do:
   - **Read** - Gives users read-only access to the data on devices in this category.
   - **Write** - Lets users read and write data to devices in this category.
   - **Execute** - Lets users run software on devices in this category.
   - **Network Share** - Gives users access to devices (CD or DVD drives) shared on the network.
5. Click OK.

Exceptions for Specified Non-Encrypted Devices

All devices that are inserted into an Endpoint Security client computer on your network show in Discovered Devices in My Organization. You can see this list in Media Encryption & Port Protection Policy > Advanced > Not Encrypted Media Access.

You can configure exceptions for:

- A narrow category of devices, for example iPods
- A model of devices, based on the device ID.
- For a specified device, based on its serial number.

For a specified device, model, or a category, select a device and click Add device as exception. When you do this the Device Properties window opens.

- **Device Serial Number** - To add that specified device as the exception, make sure there is a Device Serial Number included. You can use a wild card for the Device Serial Number to include a set of devices that have serial numbers that start with the same characters.
- **Device Name** - To add a category as the exception, delete the Device Serial Number and enter a name for the category in the Device Name field.
- **Device ID string begins with** - The Device ID represents a specified model of devices. If the Device ID is included in the Device Properties windows, all devices of that model are included in the exception. Delete the end of the string to include more devices.

For example, if the Device String is `USBSTOR\DiskSanDisk_Sansa_m240`, more devices are included than if the string is `USBSTOR\DiskSanDisk_Sansa_m240_____1.30`.

If a Device Serial Number is also in the Device Properties window, the exception includes devices that contain both the Device ID String and Device Serial Number.

If a device has not been inserted into an endpoint client in your network, it is best to insert it before you do this procedure. If Endpoint Security does not let you open the device, it will still show in the Discovered Devices in My Organization list.
To configure exceptions for a specified device:
1. In the Media Encryption & Port Protection Policy tree, select Advanced > Not Encrypted Media Access.
2. Make sure that Control Access to Non-encrypted Removable Media and Peripheral Devices is selected.
3. Select a device in one of these ways:
   - From the Devices discovered in My Organization list or from Monitoring tab > Media Encryption & Port Protection, right-click on a device, and select Add device as exception.
   - To browse to a device, for example, to find a serial number, in the Exceptions for Device Access area click the arrow on the Add button and select Add Existing.
   - To add a new device that was not inserted, go to the Exceptions for Device Access area. Click the arrow on the Add button and select Add New.
4. Select the new device and click Edit.
5. Edit the information in the Device Properties window.
   If you inserted a device, the Device Serial Number is automatically downloaded from the inserted device.
   - If a serial number is there: The exception is for the specified device.
   - If there is no serial number or if you delete the given serial number: The exception is for the category of the device.
6. In the Device ID string begins with field, you can keep the full string or delete part of it. This creates an exception category for a model of devices that start with that string.
7. Optional: Click Advanced to configure more options. These options are configured automatically based on the type of device and. It is not necessary to change them.
   - Device Capabilities - Select specified tasks that the device can do physically (not based on permissions). For example, a printer cannot be read-only, while a disk can.
   - Default device access rights - The default access for users who use the device.
   - Generate device arrival audit event - If selected, the device generates a log when it is inserted. This can only be selected if Can generate audit event on arrival is selected in the Device Capabilities area.
   - Encrypt device data with EPM - When selected, Media Encryption can encrypt this type of device. This can only be selected if Can encrypt data with EPM is selected in the Device Capabilities area.
8. Click OK.

Encrypting Removable Media

To set how media is encrypted:
1. In the Media Encryption & Port Protection Policy window, in the Encrypt Removable Media area, click Advanced Settings.
   The Media Encryption page opens.
2. Select Allow Encrypting Removable Media Devices.
3. Use the slider to set one of these encryption options:

<table>
<thead>
<tr>
<th>Encryption Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom</td>
<td>Custom settings for removable devices</td>
</tr>
<tr>
<td>Full</td>
<td>Users can:</td>
</tr>
<tr>
<td></td>
<td>• Encrypt removable media for themselves and others</td>
</tr>
<tr>
<td></td>
<td>• Remove the encryption from the encrypted device</td>
</tr>
<tr>
<td></td>
<td>• Change the size of the existing encrypted media</td>
</tr>
<tr>
<td>Medium</td>
<td>Users can:</td>
</tr>
<tr>
<td></td>
<td>• Encrypt removable media for only themselves</td>
</tr>
<tr>
<td></td>
<td>• Change the size of the existing encrypted media</td>
</tr>
</tbody>
</table>
General Properties

<table>
<thead>
<tr>
<th>Encryption Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Users can:</td>
</tr>
<tr>
<td></td>
<td>- Encrypt removable media for themselves only</td>
</tr>
<tr>
<td></td>
<td>- Cannot change the size of the existing encrypted media</td>
</tr>
</tbody>
</table>

4. To set encryption for specified devices, click **Add**.
   The **Add Device to Override Encrypt Settings** window opens. By default, encryption settings go according to device category.
   a) Select a device to add to the list.
   b) Click **OK**.
   c) For each device, decide if it must be encrypted or not.

   **Note** - Use this list to exclude specified devices from encryption

5. Configure **Offline Mode Settings** for when a connection to the Endpoint Security Management server is not available:
   - If media must be protected by a password
   - If users can recover a lost password using Remote Help

6. Optional: Expand the **Advanced Settings area** to set these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy utility to media to enable media access in non-protected environments</td>
<td>Select to allow access to encrypted media on a client computer that does not have Endpoint Security installed. The EPM Explorer allows users working on such computers to access data on an encrypted device.</td>
</tr>
<tr>
<td>Protect media with password for read only access in offline mode</td>
<td>Select to allow users access to encrypted devices when the computer is offline (when its connection to the Endpoint Security Management Server is down). Users provide an offline password to authenticate and get access. You may want to select <strong>Allow users to recover their password using remote help</strong> to allow administrators to provide Remote Help to users who forget their passwords.</td>
</tr>
<tr>
<td>Allow users to change read only password</td>
<td>Lets users change their read only offline access password.</td>
</tr>
</tbody>
</table>

7. Optional: Select **Secure format media before encryption** to erase everything on the device and reformat it before encryption. Select the number of times to format the media. The more you select, the more secure the device is. But the length of time required for encryption increases with each time that the media is formatted. The **Secure format** setting applies to each device that is encrypted by a client with this policy installed.

Creating Custom Media Authorization Settings

Media Encryption & Port Protection generates a unique signature media ID. This unique ID makes sure that media authorized in other protected environments are not approved in this protected environment.

**To customize media authorization settings:**

1. In **Media Encryption & Port Protection Policy - General Properties > Scan and Authorize Removable Media** area, click **Advanced Settings**.
   The **Media Scan Configuration** page opens.
2. Select **Scan Removable Media Devices for Threats and Authorize them for Access**.
3. Click **Configure**.
   The **Media Authorization Settings** window opens.
4. Select **Enable user to authorize media** to activate these options:
## Advanced Media Log

Expand the **Advanced** category in the Media Encryption & Port Protection Policy window to open the **Media Log** category.

Media Encryption & Port Protection logs events according to the level that you select (more logs or filtered for importance and type). Log entries are initially stored on client computers and then uploaded to the server at predefined intervals. The log shows only those entries that have been uploaded to the server.

### To set the log level:
2. Select Enable Media Logs.
3. Move the Media Log Level slider:
   - **Log Full** - important events, device changes and updates, file operations.
   - **Log Medium** - important security events, device changes and updates.
   - **Log Low** - only important events.

### Setting Device Categories to Log

By default, logs are created for all detected devices.

**To set which devices are logged:**
1. In Media Log, click Device Categories.
   The Custom Log Settings window opens. Detected device categories are listed.
2. To record logs for specified device category, select the Log option.
3. To stop logging, clear the Log option.

### Creating Exceptions to Device Logging

You can remove specified devices by type or brand name from the logs. By default, the log setting goes according to the device category.

**To set device logs for specified devices:**
1. Open a policy for editing.
2. In Advanced > Media Log, click Exceptions.
   The Override Log Settings for Specific Devices window opens. Detected devices are listed.
3. Select or clear the log option
4. Click **Add** to add other devices that must not be logged.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic media authorization</td>
<td>Media Encryption &amp; Port Protection triggers supported Anti-virus software, if present on the client computer, to scan removable media for viruses. If the media is clean, it is authorized and access is granted; otherwise access is blocked. Select <strong>Allow the user to delete unauthorized files</strong> to let users clean prohibited content from the media.</td>
</tr>
<tr>
<td>Manual media authorization</td>
<td>Select to provide users with greater control over media scanning.</td>
</tr>
<tr>
<td>Allow the user to skip media scan</td>
<td>Users can bypass scanning and allow infected or unauthorized content onto the system. This option is recommended only for testing under controlled conditions.</td>
</tr>
<tr>
<td>Allow the user to delete unauthorized files</td>
<td>Users are given the option to delete infected or unauthorized content if found on the media. After the user has deleted such content, he or she is allowed access to the device.</td>
</tr>
</tbody>
</table>
Media Encryption & Port Protection User Alerts

Configure Media Encryption & Port Protection User Alerts to show users the available options when they insert a removable device into an endpoint computer. There are different settings for different scenarios. For example, a user who can encrypt a device gets a different message than a user who cannot encrypt a device.

For each scenario you can configure if a message shows, and for some, when it shows.

This table shows the different options:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Default Message and Recommendation</th>
<th>Configure to show when:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption is not required. The user has full-access and permission to encrypt.</td>
<td>You inserted a removable device. We strongly recommend that you encrypt the device to prevent data leakage. Click Encrypt to start the encryption process.</td>
<td>Device is inserted.</td>
</tr>
<tr>
<td>Encryption is required for the user to get write-access. The user has permission to encrypt.</td>
<td>You inserted a removable device. Your organizational policy requires that you encrypt the device before you can write to it. Click Encrypt to start the encryption process.</td>
<td>User tries to write to the device. Device is inserted.</td>
</tr>
<tr>
<td>The device is blocked. The user cannot access the device and cannot encrypt.</td>
<td>You inserted a removable device. Your organizational policy does not permit this device. Please remove it now. For more information, contact your security administrator.</td>
<td>Device is inserted.</td>
</tr>
<tr>
<td>The user has read-only access and does not have permission to encrypt.</td>
<td>You inserted a removable device. Your organizational policy permits read-only access to this device. For more information contact your security administrator.</td>
<td>User tries to write to the device. Device is inserted.</td>
</tr>
</tbody>
</table>

To configure User Alerts:
1. In an open Media Encryption & Port Protection policy, select Advanced > User Alerts from the tree.
2. On the User Alerts page there are settings for the different scenarios. For each:
   - Select or clear the checkbox or checkboxes to configure when the message will open for users.
   - Optional: Edit the text to change the message that users will see.
3. Click OK.

Media Encryption Sites

Each Endpoint Security Management server has a unique identifier called its Site ID. If you encrypt a removable device on an Endpoint Security client, the Site ID of the Endpoint Security Management server that the client connects to is written on the device. This prevents clients in your organization from accessing devices that were encrypted in a different organization.

When you insert the encrypted device into a client, it sends a request to the server for an encryption key. If the encryption key is not available, the client checks the device for its Site ID. If the Site ID on the device matches the Site ID of the Endpoint Security Management server or one of the trusted servers, you are prompted for a password to access the device. If the Site ID does not match, access to the device is blocked.

You can configure clients to give access to devices encrypted on additional specified Endpoint Security Management servers. For example, in a High Availability environment, add the Site ID of each Endpoint Security Management server to all of the Endpoint Security Management servers in the environment. Then the device can be accessed on clients connected to all servers that are in the environment.
This table shows what occurs when you insert an encrypted device into a client that is connected to an Endpoint Security Management server. 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>Can you access the device?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The encrypting Endpoint Security Management server</td>
<td>Get access automatically or get access after you enter the password.</td>
</tr>
<tr>
<td>An Endpoint Security Management server that is different than the encrypting Endpoint Security Management server. This Endpoint Security Management server is configured as permitted on the encrypting Endpoint Security Management server.</td>
<td>Get access after you enter the device's password, when prompted.</td>
</tr>
<tr>
<td>An Endpoint Security Management server that is different than the encrypting Endpoint Security Management server. This Endpoint Security Management server is NOT configured as permitted on the encrypting Endpoint Security Management server.</td>
<td>You cannot access the device.</td>
</tr>
</tbody>
</table>

If you upgrade from Endpoint Security R73 to this version, we recommend that you add the Site ID of the R73 server to the permitted list.

You might be able to access devices that were encrypted on the R73 server automatically, if you transferred the encryption keys of the R73 server to the new Endpoint Security Management server. See sk60502 (http://supportcontent.checkpoint.com/solutions?id=sk60502) for details.

### Configuring Media Encryption Sites

Media Encryption Sites is part of the Media Encryption & Port Protection Policy. To prevent clients in your organization from accessing devices that were encrypted in a different organization, make sure that it is enabled.

**To configure Media Encryption sites:**

1. Select a Media Encryption & Port Protection Policy and click **Edit**.
2. In the **Media Encryption & Port Protection Policy** window, from the tree select **Advanced > Media Encryption Sites**.
3. Select: **Endpoint client will allow access only to encrypted media which was encrypted by an endpoint client connected to one of the following management servers.**
4. To configure other Endpoint Security Management servers to give access to devices encrypted on this Endpoint Security Management server, click **Copy to Clipboard** to save the site ID. Add it to other Endpoint Security Management servers later.
5. To configure the Endpoint Security Management server to give access to devices that were encrypted on different Endpoint Security Management servers:
   a) Click **Add**.
   b) In the **New Management Server** window, enter:
      - **Management Server Name** - A descriptive name for the permitted server.
      - **Management Server ID** - The site ID of the permitted server. Copy the ID from that server.
6. Click **OK**.

If Media Encryption Sites is disabled, Endpoint Security clients can access removable devices that were encrypted by all Check Point Endpoint Security Management servers.

**To disable Media Encryption sites:**

1. Select a Media Encryption & Port Protection Policy and click **Edit**.
2. In the **Media Encryption & Port Protection Policy** window, from the tree select **Advanced > Media Encryption Sites**.
3. Select: **Endpoint client will allow access to encrypted media which was encrypted by an endpoint client connected to any management server.**
Converting Legacy Encrypted Devices to Media Encryption

You can easily convert USB devices that are encrypted with Pointsec Media Encryption (PME) or Check Point File Encryption (FE) to Media Encryption. When you insert a USB device encrypted with PME or FE into an Endpoint Security computer with Media Encryption & Port Protection, on-screen instructions show you what to do.

**To convert a legacy encrypted USB device to Media Encryption:**

1. Insert the device into a computer that has an Endpoint Security client with Media Encryption & Port Protection installed.
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 are the credentials that were used originally when the device was encrypted. They can be:
   - A corporate username and password that the administrator tells employees.
   - A personal username and password for the device
   If the device was originally encrypted with the 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**.

Changing the Group Ranking Order

You can change the group ranking order of a node to make sure that users in multiple groups receive the correct Media Encryption & Port Protection Policies.

For example, you have a user who is in the Team Leader group and the Developer group, which have different policies. The user must receive the policy of the Team Leader group. Do this by placing the Team Leader group above the Developer group in the rankings.

**To edit the group ranking order of nodes:**

Select **Policies** tab > Media Encryption & Port Protection.

1. In the **Media Encryption & Port Protection Policy Overview** window, select **Assignments** from the **View By**: drop down box.
2. Click **Group Assignment Priority**.
3. In the **Group Assignment Priority** window, select **Use global group assignment priority ranking** or **Override group assignment priority**.
4. Select a node
5. Use the up and down arrows to move the node to a position with higher priority.
6. Click **OK**.
Firewall Rules Policies

Firewall rules allow or disallow network traffic based on connection information, such as IP addresses, ports, and protocols. For Endpoint Security management, two types of firewall rules are available:

- **Inbound rules** - rules that allow or disallow incoming network traffic to the endpoint computer (known as localhost).
- **Outbound rules** - rules that allow or disallow outgoing network traffic from the endpoint computer.

**Note** - The firewall policy is affected by Endpoint compliance states ("Non-Compliance" on page 61), and whether the Connected or Disconnected ("Enforcing Policies According to States" on page 61) policy is in force.

In This Chapter

- Firewall Rules Policy Options
- Firewall Rules - Control Icons and Buttons
- Firewall Rule Number
- Creating Firewall Rules
- Advanced Settings

Firewall Rules Policy Options

To Configure Firewall Rules:
1. Click Policies tab > Firewall Rules blade.
2. To edit an existing policy, select it in the table and click Edit.
   To define a new policy, click New.
   The Firewall Rules window opens.
3. Use the options in this window to:
   - Add, edit, or remove rules from the policy
   - Add, edit, or remove new Network objects and services.

Firewall Rules - Control Icons and Buttons

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO.</td>
<td>Firewall Rules are enforced from the top of the table to the bottom. The last rule is usually a Cleanup Rule. The last rule says drop. Traffic that fails to match any of the previous rules is terminated by the Cleanup Rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Firewall Rule.</td>
</tr>
<tr>
<td>Source and Destination</td>
<td>Source and Destination can be any of the Network Objects defined in the Access Zones policy or the Trusted/Internet Zone.</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Source location of network traffic. For an outbound rule, the source will always be the <strong>LocalComputer</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Destination location of network traffic. For an inbound rule, the destination will always be the <strong>LocalComputer</strong>.</td>
</tr>
<tr>
<td>Service</td>
<td>Network protocol or service used by traffic.</td>
</tr>
<tr>
<td>Action</td>
<td>Effect of the rule on matched traffic: <strong>Accept</strong> or <strong>Drop</strong>.</td>
</tr>
<tr>
<td>Track</td>
<td>Record Endpoint Security client behavior when the rule is enforced:</td>
</tr>
<tr>
<td></td>
<td><strong>Log</strong> - record rule enforcement in the Endpoint Security client log.</td>
</tr>
<tr>
<td></td>
<td><strong>Alert</strong> - display pop-up on the endpoint computer and record rule enforcement in the Endpoint Security client log.</td>
</tr>
<tr>
<td></td>
<td>Note: For tracking to work, Firewall logs must be enabled in the Common Client Settings policy.</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> - log and alert messages are not generated.</td>
</tr>
<tr>
<td></td>
<td>If you have a rule that drops or accepts all traffic, do not enable logging.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon/Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Rule at the Bottom</td>
<td>When adding rules to the Firewall policy, remember that rules at the top of the table are evaluated against traffic before rules at the bottom. To make sure that a rule is evaluated only after all other rules have been evaluated, add it to the bottom. Once the rule is located in the proper place, decide whether the rule applies to inbound or outbound traffic.</td>
</tr>
<tr>
<td>Add Rule at the Top</td>
<td></td>
</tr>
<tr>
<td>Add Rule below Current</td>
<td></td>
</tr>
<tr>
<td>Add Rule above Current</td>
<td></td>
</tr>
</tbody>
</table>

| (To move a rule)       | Drag and drop rules to change the behavior of the firewall by changing the order in which rules are matched to traffic.                |
| (To remove a rule)     | To remove a rule, right-click the rule > Delete Rule.                                                                                 |
| (To add a new rule)    | To create a new rule (Host, Address Range, Site or Network):                                                                         |
|                        | • Right-click the table heading row of General Properties > New Rule > Inbound or Outbound. A new Inbound or Outbound rule is added at the top of the table of rules. |
|                        | • Right-click a rule row > New Rule > Inbound or Outbound > Above or Below. The new Inbound or Outbound rule is added to the current row. |
| Edit                   | After modifying a firewall rule, the policy must be installed on the Endpoint before it takes effect.                               |
|                        | Note:                                                                                                                                  |
|                        | • Endpoint Security Management Console and SmartDashboard make use of the same network objects in the database. Changing an object's properties in the Endpoint Security Management Console affects how the object behaves in SmartDashboard. |
|                        | • This is also true for Firewall Rules policies that use the same object. Changing the object's properties for one policy changes how the object behaves in all other Firewall Rules policies. |
Firewall Rule Number

In a security policy, the rule number (NO.) indicates the order in which a client evaluates the firewall rules. The rule at the top of the table is tested first. For this reason, rule order is important.

Examples of Rule Numbers

Consider the following FTP rules:

- **FTP Local** allows FTP clients from the local private subnet to connect to the protected computer’s FTP server.
- **FTP Internet** blocks all FTP clients from connecting to the protected computer’s FTP server.

**Example 1**

Accept incoming local FTP traffic and drop other traffic

<table>
<thead>
<tr>
<th>NO.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FTP Local</td>
<td>Private Subnet</td>
<td>LocalMachine</td>
<td>FTP</td>
<td>Accept</td>
<td>Log</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>FTP Internet</td>
<td>Any</td>
<td>LocalMachine</td>
<td>FTP</td>
<td>Drop</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**FTP Local** is rule 1 and **FTP Internet** is rule 2.

- FTP requests from clients on the local subnet match all the conditions of the **FTP Local** rule. Client accepts FTP traffic.
- FTP requests from clients outside of the local subnet do not match **FTP Local**.
  - **FTP Local** is not run.
  - The client checks the next rule.
  - The traffic matches the conditions of **FTP Internet**.
  - The client runs **FTP Internet**.
  - Client drops FTP traffic.

**Example 2**

Dropping all incoming FTP

<table>
<thead>
<tr>
<th>NO.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FTP Internet</td>
<td>Any</td>
<td>LocalMachine</td>
<td>FTP</td>
<td>Drop</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Creating Firewall Rules

FTP Internet is rule 1 and FTP Local is rule 2.

- All FTP requests from clients on the local subnet and other all locations match the FTP Internet rule.
- Client runs FTP Internet
- Client drops FTP traffic

Note - While FTP Internet remains at the top of the table, FTP Local is never evaluated. Traffic always matches the conditions of the first rule.

Creating Firewall Rules

To create a Firewall rule:
2. Enter the Name of the policy and a Comment.
3. To create a new rule, right-click in the pane and select New Rule. The rule is placed at the top and assigned NO. 1.
4. To move the rule: drag and drop.
5. To add a name, right click the Name column and select Edit.
6. Enter the name in the Name window.
7. To add a network object to the Source column, drag the object from the Network Objects tab.
   a) Alternatively, right-click the Source column and select Add.
   b) Select the network object from Available Objects in the Add Object window.
   c) Click Add> to move it to Selected Objects.
8. To add a network object to the Destination column, drag the object from the Network Objects tab.
   a) Alternatively, right click the Destination column and select Add.
   b) Select the network object from Available Objects in the Add Object window.
   c) Click Add> to move it to Selected Objects.
9. To add a service to the Service column, drag the service object from the Services tab.
   a) Alternatively, right click the Service column and select Add.
   b) Select the network object from Available Objects in the Add Object window.
   c) Click Add> to move it to Selected Objects.
10. To specify the Action, right-click the action cell and select accept or drop.
11. To specify the type of tracking, right click the Tracking cell and select Alert, Log, or None.
12. To specify a comment, right click the Comment cell, select Edit, and enter text in the window.

To create a Network Object on the Network Objects tab:
1. Click New.
2. Select the type of object:
   - Host
   - Address Range
   - Network
   - Site.
3. Click OK.
4. In the Properties window, enter the needed data: Name, IP address.
5. Click OK.

To create a Service on the Services tab:
1. Click New.
2. Select the type of service: TCP, UDP, or Group.

3. Click OK.
   - In the Service Properties window, specify the Name, Port, Color, and Comment. Or:
   - In the Group Properties window, add Available Services to a group.

4. Click OK.

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.

Advanced Settings

In the Firewall Rules Policy > Advanced Settings, you can configure these settings:

- **Disable Wireless On LAN** - The Disable Wireless on LAN feature prevents endpoint users from connecting to unauthorized wireless networks while on your organization’s LAN. This protects your network from threats that can come from wireless networks.
  - If selected - Users cannot connect to unauthorized wireless network while on your organization’s LAN.
  - If cleared - Users can connect to unauthorized wireless network while on your organization’s LAN.

- **Allow Hotspot Registration** - Some firewall policies do not permit use of hotspots for users who want to connect to your network from a hotel or public place. The Enable Hotspot Registration feature lets users connect to your network from a hotspot and also controls the parameters of hotspot-specific port openings. This feature is integrated with the Endpoint Security VPN blade.
Chapter 15

Access Zones Policies

Access Zones Definitions lets you to create discrete security zones for use in Application Control and Firewall Rules. For this reason, configure Access Zones before configuring Application Control and Firewall Rules.

There are two Access Zones:

- The Internet Zone
- The Trusted Zone

Network locations not placed in the Trusted Zone automatically belong to the Internet Zone.

In This Chapter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Zone</td>
<td>117</td>
</tr>
<tr>
<td>Network Objects</td>
<td>118</td>
</tr>
<tr>
<td>Creating New Access Zones Definitions</td>
<td>121</td>
</tr>
<tr>
<td>Changing an Existing Access Zones Policy</td>
<td>121</td>
</tr>
</tbody>
</table>

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.

The Endpoint Security Management Console 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 Application Control and Firewall Rules policies. For example, in the Application Control policy, access permissions are granted for each application or applications group when accessing the Trusted Zone or the Internet Zone. If the initial Access Zones policy is used in an Application Control policy, then the idea of an Internet Zone has no meaning. The Internet Zone is the same as the Trusted Zone.

- **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.

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.

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.

Adding Network Objects

You can add network objects to the Available Network objects list.

To add a network object:
2. Click New.
   The Access Zones Definitions Policy window opens on the General Properties page.
3. Click New.
4. The Select New Object Type window opens.
   Each object in the list represents a network object.
5. Select an object type from the list.
6. Click OK.
   The Properties window for the selected object opens.
7. Enter the needed data to define an object of one of the these types:
   - Host ("Configuring a Host as a Network Object" on page 119)
   - Address Range ("Configuring an Address Range as a Network Object" on page 119)
   - Network ("Configuring a Network as a Network Object" on page 119)
   - Site ("Configuring a Site as a Network Object" on page 120)
- Group ("Configuring a Group as a Network Object" on page 120)
- Network Group with Exclusion ("Configuring a Network Group With Exclusion" on page 120)
- Site Group ("Configuring a Site Group as a Network Object" on page 121)

8. Click OK.
9. Select the object you created, and click the Add button of Trusted Zone Objects. The object is added to the list you selected.

### 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 **New**. The **Group Properties** window opens.

3. Select from the **Available Objects** column, or create a new object of the type:
   - Host
   - Address Range
   - Network
   - Group
   - Network With Exclusion

**Configuring a Network Group With Exclusion**

Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Object in</td>
<td>Select a group in which the network object should reside from the drop-down list.</td>
</tr>
<tr>
<td>Except</td>
<td>Select an exception (where the network object should not reside) from the drop-down list.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network object.</td>
</tr>
</tbody>
</table>
**Configuring a Site Group as a Network Object**

1. Enter data that defines the network object:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network object.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network object.</td>
</tr>
</tbody>
</table>

2. Select **New**. The **Site Group Properties** window opens.

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

---

**Creating New Access Zones Definitions**

Create new **Access Zones Definitions** in which network objects are assigned to the security zone.

**To create a new Access Zones Definition:**

1. Select **Policies** tab > **Access Zones Definitions**
   The **Access Zones Definitions Policy Overview** window opens. Make sure **Policies** displays in the **View By:** drop-down list.
2. Click **New**.
3. The **General Properties** window opens.
4. Enter the needed information:

<table>
<thead>
<tr>
<th>Policy Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the policy.</td>
</tr>
<tr>
<td>Color</td>
<td>A color to be used for the icon for this policy from the drop-down list.</td>
</tr>
<tr>
<td>Comment</td>
<td>A description of the policy.</td>
</tr>
</tbody>
</table>

5. Create network objects ("Adding Network Objects" on page 118).
6. Add network objects to **Trusted Zone Objects** by
   - Selecting a network object from the **Available Network Objects**
   - Clicking the **Add** arrow
7. Click **OK**.

**Note** - You cannot reliably use hostnames (such as Google or MSN) to restrict sites that have multiple IP addresses.

---

**Changing an Existing Access Zones Policy**

You can change attributes of existing Access Zones Rules **Policy** by adding or changing network objects, and Trusted Zone objects for an Access Zones policy.

**To change an existing Access Zones Policy:**

1. Select **Policies** tab > **Access Zones Rules**.
   The **Access Zones Rules Policy Overview** window opens. Make sure that **Policies** displays in the **View By:** drop-down list.
2. Select the policy to change from the list, and click Edit.

3. The General Properties window opens.

4. To make changes in the Name field and Comments field, delete the existing text and enter the new text.

5. To change the color used to identify the policy, use the color drop down list.

6. To add an existing object to the Trusted Zone Objects list:
   - Select a network object from Available Network Objects
   - Click the Add arrow

7. To remove an existing object:
   - Select the network object from the list
   - Click the Remove arrow

8. To delete an existing object, select the object and click Delete.
Chapter 16

Malware Protection Policies

Check Point Malware Protection protects your network from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers. Use Malware Protection to centrally manage the detection and treatment of malware on your endpoint computers.

The Endpoint Security Management Server regularly receives updated Anti-malware definitions from a Check Point update server.

In This Chapter

Prerequisites 123
Malware Protection - Settings 124

Prerequisites

Before configuring Malware Protection, do these steps.

Configuring a Proxy Server

As a part of planning your environment for Malware Protection, you need to configure a proxy server. This section describes how to configure proxy servers in a Windows environment.

To configure a proxy server in Windows:
2. Open:
   C:\Program Files\CheckPoint\CPuepm\80.20\engine\conf\local.properties
3. Add these properties:
   a) Specify the proxy server's IP address as shown in the example below:
      http.proxy.host=123.456.78.90
   b) Specify the proxy server's listening port as shown in the example below:
      http.proxy.port=8080
   c) Specify the username if basic authentication is enabled on the proxy server. Leave it empty if no authentication is required.
      http.proxy.user=<username>
   d) Specify the password if basic authentication is enabled on the proxy server.
      http.proxy.password=<password>
4. Save the local.properties file.

Enabling Update Traffic

After configuring the proxy server, set up the firewall gateway to accept the traffic to and from 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 inbound and outbound connectivity to the Anti-virus update server.
Port Access

- Endpoint Security server must have access to ports 80 and 443 to retrieve the latest virus and spyware information. Make sure that your firewall gateway allows this traffic.

- If you plan to use Malware Protection in an environment that includes a proxy server for Internet access, configure Endpoint Security server to work with a proxy server.

Malware Protection - Settings

Malware Protection detects and treats viruses (both dormant and active) on the endpoint computer. Files are scanned when accessed directly by users or indirectly by other processes.

Quick Start


These Malware Protection policies are available:

- **High Security Malware Protection Policy** - Default settings for high level security.
- **Medium Security Malware Protection Policy** - Default settings for medium level security.
- **Low Security Malware Protection Policy** - Default settings for low level security.
- **Off Malware Protection Policy** - Default settings for no malware security.

To assign a policy:

   - The Malware Protection Policy Overview page opens.
2. Double-click one of the predefined policies.
   - The Malware Protection Policy window opens.
3. Click Assignment.
4. On the Assignment window, click Add Assignment and select nodes from the Navigation tree.
5. Click OK.
   - The assignment is shown on the Assignment window.
6. Click OK.

Creating a Malware Protection Policy

If you require different settings than the predefined policies, you can create a new policy.

**To add a new malware protection configuration:**

   - The Malware Protection Overview page opens.
2. Click the View By drop-down box, and select Policies.
3. Click New.
   - The Malware Protection Policies window opens.
4. Configure the Malware Protection settings.
5. Click OK.

Viewing Malware Protection Assignments

You can see all Malware Protection Policies assignments. Single or multiple Policies can be assigned to the organization or directories, groups, users, and endpoint computers within the organization.
To show policy assignments:
1. On the Malware Protection Overview page, click the View By drop-down box
2. Select Assignments.

# Malware Protection Settings

This section describes the Malware Protection settings that protect endpoint computers against all types of malware.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Level Settings</strong></td>
<td>Select from these scan levels:</td>
</tr>
<tr>
<td>- Custom</td>
<td>Applies settings configured in the Custom Scan Level Settings window (“Custom Scan Level Settings” on page 126).</td>
</tr>
<tr>
<td>- Low Scan Level</td>
<td>Scans only the critical areas of the computer, for example, the operating system, processes, and memory. These are the targets of most malicious programs and it is critical to protect them.</td>
</tr>
<tr>
<td>- Medium Scan Level</td>
<td>Scans all critical areas.</td>
</tr>
<tr>
<td>- High Scan Level</td>
<td>Scans all critical areas.</td>
</tr>
<tr>
<td></td>
<td>Scans all files on the computer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Scan Schedule Settings</strong></th>
<th>Select from these scan schedule options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Scan monthly</td>
<td>Schedules one scan a month at the specified time.</td>
</tr>
<tr>
<td>- Scan weekly</td>
<td>Schedules one scan a week at the specified time.</td>
</tr>
<tr>
<td>- Scan daily</td>
<td>Schedules a scan every day at the specified time.</td>
</tr>
</tbody>
</table>

Click Configure to set a date for the first scan and the time of day that scans will occur.

<table>
<thead>
<tr>
<th><strong>Scan Treatment Settings</strong></th>
<th>Select how Endpoint Security handles infected files:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Repair the file. If repair fails, delete</td>
<td>If Endpoint Security cannot repair the file it deletes it.</td>
</tr>
<tr>
<td>- Repair the file. If repair fails, quarantine</td>
<td>If Endpoint Security cannot repair the file it quarantines it. The file is deleted and put in a secure location from where it can be restored if necessary.</td>
</tr>
</tbody>
</table>
## Malware Protection - Settings

### Exclude Directories and Trusted Processes

Select this option to exclude specific directories, files or file types from the malware scan and to prevent monitoring of trusted processes. Click **Advanced Settings** (*Malware Protection - Scan Exclusion and Processes* on page 127) to add:

- 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.

**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.
- The chosen items are excluded from on demand, scheduled, and on access scans. They are not be excluded from user triggered scans (right click > Scan with Check Point Anti-Malware).

### Signature and Engine Update Settings

Configure the frequency, in hours, between client requests for malware signature updates or select the update source. Click Advanced Settings (*Malware Protection - Engine & Signature Updates* on page 127) to select:

- A malware signature update server.
- An update connection time out.

### Custom Scan Level Settings

Customized Malware Protection scan level settings give you greater control of file and drive types.

**To customize scan level settings:**

1. Open a Malware Protection policy for editing
2. On the **General Properties** page > **Scan Level Settings** click **Configure**.

The **Custom Scan Level Settings** window opens:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan File Types</strong></td>
<td>Select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• Quick Scan  Scans the Windows folder, subfolders, and startup items.</td>
</tr>
<tr>
<td></td>
<td>• Normal Scan   Scans all files except compressed files and non-executable files.</td>
</tr>
<tr>
<td></td>
<td>• Deep Scan    Scans all file types.</td>
</tr>
<tr>
<td><strong>Scan Targets</strong></td>
<td>Select from these scan targets:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Removable</strong> - Scans removable media devices, such as USB.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CD-ROM</strong> - Scans CD-ROMs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Other</strong> - Any device which Windows recognizes as a drive.</td>
</tr>
<tr>
<td></td>
<td>Note: By default, the local drive is always selected.</td>
</tr>
<tr>
<td><strong>Do not scan files larger than</strong></td>
<td>Do not include files above a certain size if scanning them significantly decreases computer performance.</td>
</tr>
</tbody>
</table>
Malware Protection - Settings

**Optimize Scan time by storing file checksums and NTFS file system data**
Optimize the scan by storing file checksums and NTFS file system data during the first scan. NTFS cluster size, file name, and folder structure are cached. During subsequent scans, only new files or files whose checksum, file size, name, or structure has changed are scanned.

---

**Malware Protection - Engine & Signature Updates**

You can define the frequency, in hours, between client requests for malware signature and scanning engine updates.

**To define the update frequency:**
1. Go to the Malware Protection Policy window.
2. Open an existing policy or create a new policy.
3. In the General Properties pane, enter or select the number of hours between update requests. The default is an interval of four hours.
4. Click Advanced Settings.
5. In the Signature and Engine Update Settings pane:
   - Select Update from the Endpoint Server to get updates for the specified Endpoint Security server.
   - Select Update from external source to get updates from a predefined URL. Enter the URL in the specified field.
     If you select the two options, the client first tries to get updates from the Endpoint Security server. If the server is unavailable, the client downloads updates from the external source.
   - Enter or select a timeout period, in seconds, in the designated field.
     The timeout period defines the period after which the Endpoint Security server is considered to be unavailable.
6. Click OK.
   The trusted directory now shows in the Scan exclusions list.

---

**Malware Protection - Scan Exclusion and Processes**

You can exclude the contents of trusted directories or files and specified trusted program executables from the Malware Protection 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 Malware Protection. Only exclude a process 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.

**To exclude a directory or file from real-time protection:**
1. Go to the Malware Protection Policy tab. window.
2. Open an existing policy or create a new policy.
3. In the General Properties pane, select the Exclude Directories and Trusted Processes option.
4. Click Advanced Settings or select Scan Exclusion and Trusted Processes from the tree.
5. On the Scan Exclusion and Trusted Processes page, below the Scan exclusions list, click Add.
6. In the Path Exclusions window, click Browse and go to the trusted directory. Alternatively, you can:
   - Enter a directory path.
   Example: C:\Program Files\MyTrustedDirectory\
- Enter a specific file
  Example: C:\Program Files\excludeMe.txt
- Enter a file type
  Example: *.txt

Note - Do not use environment variables to exclude folders and file paths.

7. Click OK.
   The trusted directory shows in the Scan exclusions list.

To exclude a trusted program executable or process from a scan:
1. Go to the Malware Protection Policy window.
2. Open an existing policy or create a new policy.
3. In the General Properties pane, select the Exclude Directories and Trusted Processes option.
4. Click Advanced Settings or select Scan Exclusion and Trusted Processes from the tree.
5. In the Scan Exclusion and Processes pane, below the Trusted Processes list, click Add.
6. 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
7. Click OK.
   The trusted program shows in the Trusted Processes list.

Malware Protection - Assignment Settings

Do these steps to assign a Anti-malware policy.

To assign a policy:
1. In the Policies tab, in the Overview page of a blade, open an existing policy or create a new one.
2. The Policy window opens.
3. Click Assignment in the navigation tree.
4. Click Add Assignment.
   The Select Node window opens.
5. In the Navigation Tree, select a node in the directory. When you select a directory or group, users that belong to that group or directory show in the Node area.
6. Click OK.
7. On the Assignment page, click the Add Assignment down arrow, and select from the displayed options.
8. Click OK.
9. Click Install Policies.

To assign a different policy:
1. On the Assignment page, select the node row and click the Assign Different Policy down arrow.
   The list of policies is shown.
2. Select a policy.
3. Click OK.
4. Click OK.
5. Click Install Policies.
Chapter 17

Application Control Policies

Application Control restricts network access of applications that act as either clients or servers. An Application Control policy includes a set of access permissions for programs.

In This Chapter

Creating Application Control Configuration 129
Understanding Application Groups 129
Permissions 130
How Application Control Functions 132
Planning Application Control 133
Monitoring Applications - Automatic Add 136
Creating Custom Program Groups 136
Changing Group Definitions 137
Deleting Program Groups 137
Managing Unknown Applications 137
Program Permissions and Disconnected Policies 138
Importing Programs 138
Manually Adding Programs 141
Program Advisor 141

Creating Application Control Configuration

You can create as many Application Control configurations as you need. For example, users may need access to remote administration applications that the general population does not have access to.

To create a new configuration for policies:

1. In Policies tab > Application Control, click New.
   The Program Control Policy - New Program Control Policy window opens.
2. Provide a name and optional comment and color to identify this configuration.
3. Make sure Enable Application Control is selected.
   The Program Rules list shows the existing program groups and their permissions. Permissions in gray are inherited by default settings. Permissions in color are overrides.
4. Open the Assignment tab to see which nodes in the My Organization tree are assigned to this configuration.
   This tab may be empty when you first create the configuration.
5. Open the Programs tab to see the programs that are observed by Endpoint Security.
   When an endpoint runs a program that attempts to access a network or Internet connection, it is added to this list. This tab may be empty when you first create the configuration.

Understanding Application Groups

Endpoint Security will observe numerous applications running on your endpoints. To provide efficient application management, they are added to application groups.

Check Point provides the following main default application groups:
Permissions

Note - If you do not see the PA groups, ask your Check Point distributor about obtaining a Program Advisor subscription.

Table 17-1 Default Application Groups

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Description of Contained Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA terminated applications</td>
<td>Applications that Program Advisor recommends terminating because they are known to be malicious.</td>
</tr>
<tr>
<td>Critical Services</td>
<td>Applications that must have these permissions, or the endpoint will not function correctly. For example: LSASS and svchost.</td>
</tr>
<tr>
<td>Secondary Services</td>
<td>Services and applications that should have these permissions for correct functioning.</td>
</tr>
<tr>
<td>PA referenced Applications</td>
<td>Applications that Program Advisor recommends allowing.</td>
</tr>
<tr>
<td>Unknown Applications</td>
<td>Applications that are not governed by any other group. You should monitor this group frequently and make sure that applications are moved out this group (filters are created for other groups that will pull in matching applications from this group).</td>
</tr>
</tbody>
</table>

There are also predefined application groups for specific application types, such as Mail Clients and Browsers.

Custom Groups

You can create custom groups. Custom groups act as filters, grouping applications together according to the criteria you specify.

Some possible uses for custom groups include:

- Grouping by publisher - Use this option when you want to apply the same permissions to all software from the same company.
- Grouping by file name - Use this option to apply the same permissions to all versions of an application. This is useful when your users are using many different version of the same application, such as Microsoft Outlook. You can also use this for applications that change checksum frequently, such as applications that your organization is creating.

Permissions

Permissions control application access on endpoint computers. Permissions should be applied to Program Groups in most cases. You can override the group permissions for specific programs, but it more efficient to set permissions for groups. This efficiency may include performance of Endpoint Security policies on the clients as well as administrator maintenance demands.

Permissions are applied according to where and how the program is attempting to access.

- **Access Zone** - Traffic is evaluated by the computer or server that the program is trying to communicate with, according to the zones you define in the Access Zones Software Blade configuration. Programs that attempt to contact a location that is not in one of these zones are always blocked. You can set permissions for communication to and from the Trusted Zone, and to and from the Internet Zone (which includes all locations that are not defined in the Trusted Zone).
- **Role** - Traffic is evaluated according to whether the program is trying to establish a connection (acting as a client) or to listen for a connection (acting as a server).

Permission settings may be one of the following:

- **Allow** - Allows the program to establish or accept the connection.
• **Block** - Blocks the program from establishing or accepting the connection.
• **Terminate** - Denies the connection and terminates the program.

Therefore, the possible permissions for a program are:

**Table 17-2 Permission Options**

<table>
<thead>
<tr>
<th>Zone + Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted + Client</td>
<td>Permission of program on endpoint computer to connect to a server that is in the defined Trusted Zone. For example, Outlook permissions to connect to an Exchange server. <strong>Allow</strong> is the usual setting for this zone and role.</td>
</tr>
<tr>
<td>Trusted + Server</td>
<td>Permission of program on endpoint computer to listen for clients in the Trusted Zone and provide a service. For example, FTP services on a managed FTP server.</td>
</tr>
<tr>
<td>Internet + Client</td>
<td>Permission of program on endpoint computer to connect to a server that is in the Internet Zone. For example, Firefox permissions to access Google; Yahoo Instant Messenger to access Yahoo Services.</td>
</tr>
<tr>
<td>Internet + Server</td>
<td>Permission of a program on endpoint computer to listen for clients outside the trusted zone and provide a service. <strong>Block</strong> is the usual setting for this zone and role.</td>
</tr>
</tbody>
</table>

**Permission Precedence**

Program access is moderated according to the permissions of the first group it belongs to. Groups are ranked in the following order:

- PA (Check Point Program Advisor) terminated programs
- Custom groups, in the order they appear in the Program Groups window.
- PA referenced programs
- Unknown programs

You change the order (and thus the precedence) of your custom groups.

**To change precedence of program groups:**
1. Open Policies tab > Program Control > Program Groups.
2. Select the program group whose precedence you want to change.
3. Drag and drop the program group to the desired position in the program groups list.
   For example: assume you have two groups: Browsers and Firefox Browsers. You set the permissions of the Browsers group to Block Server actions on both Trusted and Internet Zones. You set the permissions of Firefox Browsers to Block Server actions on only the Internet Zone. An endpoint using Firefox will get the permissions of the group that opens first in the list.
   - If Browsers is above Firefox Browsers, the endpoint cannot use Firefox as a server at all.
   - If Firefox Browsers is above Browsers, the endpoint can use Firefox as a server to trusted computers.

**Editing Program Group Permissions**

You can change the permissions of a group at any time. All programs in a group inherit the permissions of the group (permissions shown in gray), unless you override the permissions for specific programs (permissions shown in color).
To edit program group permissions, by policy:
1. Open Policies > Application Control, select a policy and click Edit.
   The Application Control Policy window opens, with General Properties displayed.
2. Right-click a program group and select Override.
   The Edit Program Group Permissions window opens.
3. Make sure that the Override global permissions check box is selected, and set the permissions for this group.

To edit program group permissions, for all policies:
1. Open Policies > Application Control > Program Groups.
2. Double-click a program group.
   The Program Group window opens.
3. Change the Group Permissions settings.

Editing Specific Program Permissions
You can set individual permissions for a program, overriding the permissions of the group. Generally, for maximum efficiency you should set permissions on the group level whenever possible and only make exceptions when absolutely necessary.

To override permissions for a program, by policy:
1. Open Policies > Application Control, select a policy and click Edit.
   The Application Control Policy window opens.
2. Open the Programs category.
3. Right-click the program you want and select Override.
   The Edit Program Permissions window opens.
4. Select Override global permissions and set the permissions for this program.

To override permissions for a program, for all policies:
1. Open Policies > Application Control > Program Groups.
2. Right-click a program group and select Edit Programs.
   The Programs window opens.
3. Double-click the program.
   The Editing Program Permissions window opens.
4. Set the permissions for this program.

How Application Control Functions
The Endpoint Security client contacts the Endpoint Security Management Server for Application Control permissions in the following process.

1. An application or service starts on the endpoint, requests network access, and is observed by the endpoint.
2. The client checks for locally stored permissions.
   If permissions are found on the client, the program is allowed, blocked, or terminated according to those permissions.
3. If the permissions are not found locally, the client checks with the Endpoint Security Management Server.
   • If permissions are on the Endpoint Security Management Server, the program is allowed, blocked, or terminated accordingly.
   • Otherwise, the Program Advisor server is contacted and its permissions are used.
4. If the program is unknown, the permissions of the Unknown Programs group are applied.
   In addition, if the client cannot reach the servers, and the program is newly observed to request network access, the permissions of Unknown Programs are applied.
Planning Application Control

Take into account the following functionality when planning your configurations of the Application Control Software Blade.

- Pay particular attention to the settings you apply to Unknown Applications.

  **Important** - When the Endpoint Security client cannot contact the Endpoint Security Management Server, and a new application attempts network access, it is always given the permissions of the Unknown Applications group.

- You can start with Black Listing - allow application groups that are not terminated or blocked by default and block application groups as the need arises. For example, you may decide to allow all users to use Skype in the beginning and later decide to block a video-streaming instant messengers group, to ensure greater bandwidth for everyone.

- You should plan to reach White Listing - block all applications except those you explicitly allow. You achieve a high level of security, but may have to handle permission and group changes to ensure endpoint user productivity. The more maintenance you put in during Black Listing, the better your White Listing will work for your organization.

- It is recommended that the setting **Enable for Disconnected Policies** be selected only for critical application groups. This setting enlarges the policies, both Connected and Disconnected, and can adversely affect performance.

- Be aware that Check Point Program Advisor service provides professionally-recommended security settings for most applications.

**Program Permission Lifecycle Use Case**

Each program behavior carries a different level of risk. To avoid causing needless disruption to your users, you should plan your program permissions according to the risks involved and your organization’s security needs.

It is recommended that you begin your implementation with a permissive policy, that uses lenient and less disruptive program permissions and later tighten your security with progressively more restrictive policies: that you go from Black Listing to White Listing. If possible, it is recommended that you go through this cycle in a lab environment before moving to production.

The recommended flow is:

1. Allow Internet + Server (allows all) as default.
2. Monitor observed programs and block Internet + Server permissions for programs that should not be providing services to outside clients.
   You can change the permissions by policy, so that a server in your company has different program permissions than do your user desktops.
3. Monitor again, and block Internet + Client for programs that should not be allowed to connect to outside sources.
4. Monitor again. If programs are observed to be acting as servers to clients within the Trusted Zone, and you want to block this behavior, set Trusted + Server to Block.
5. If there remain programs whose running or network access you want to restrict entirely, set Trusted + Client to Block.

**Unknown Program Configuration - Use Case**

This example shows how to implement the recommendation to start with less disruptive (more lenient) permissions for Unknown Programs, and gradually monitor and change to more secure.

Each phase in the use case is evaluated for the following criteria:

- **Unknown attack protection** - How effectively does the configuration protect against unknown attacks?
- **User restriction** - How much does this restrict what the end user can do?
- **Maintenance** - How much time will you have to spend adding exceptions and specific program permissions?

### Table 17-3 Unknown Program Permissions - Use Case

<table>
<thead>
<tr>
<th>Lifecycle of Permissions of Unknown Programs Group</th>
<th>Permission Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Trusted Zone</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
<tr>
<td>Phase 0: Black Listing</td>
<td>Allow</td>
</tr>
<tr>
<td>Phase 1: Block Internet Zone servers only</td>
<td>Allow</td>
</tr>
<tr>
<td>Phase 2: Block all servers</td>
<td>Block</td>
</tr>
<tr>
<td>Phase 3: Block all non-trusted communication</td>
<td>Allow</td>
</tr>
<tr>
<td>Phase 4: White Listing</td>
<td>Block</td>
</tr>
</tbody>
</table>

If possible, it is suggested that you advance through these phases of Application Control configuration in an evaluation environment, so that when you move to Production (installing the Endpoint Security client and policies on endpoints) only when you can efficiently block Unknown Programs without disrupting your users.

The time and maintenance between Black Listing and Phase 1 should be quite long. You should be analyzing usage reports and logs to determine your organization's needs and possible needs for different Application Control configurations for Endpoint Security policies.

### Phase 1: Block Internet Zone Servers Only

This is the most lenient of the sample settings for Unknown Programs. Applications that accept connections from outside sources over the Internet pose the greatest risk to the endpoint; therefore, this configuration provides effective security by blocking your endpoints from acting as servers to unknown clients.

This configuration assumes you have defined your Trusted Zone, with corporate hosts and networks. By leveraging the Trusted Zone, the few applications that need server rights to operate on the corporate network will have these by default.

### Table 17-4 Impact of Blocking Internet Zone Server Role

<table>
<thead>
<tr>
<th>Impact area</th>
<th>Level</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown attack</td>
<td>Good</td>
<td>Any unknown application that tries to accept a connection from the Internet Zone is blocked.</td>
</tr>
<tr>
<td>protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User restriction</td>
<td>Low</td>
<td>Users are able to run unknown programs that send traffic to the network and that accept a connection from a trusted host.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Low</td>
<td>You will only have to configure exceptions for applications that need to be specifically blocked from sending network traffic, or that need to accept connections on the Internet Zone.</td>
</tr>
</tbody>
</table>

### Phase 2: Block All Servers

Use these settings for Unknown Programs if you do not want any of them to act as servers, even to clients on your Trusted Zone. This increases your level of protection, but requires more maintenance and is potentially more disruptive to users if you fail to grant server permissions to legitimate programs.
### Impact of Blocking Servers

<table>
<thead>
<tr>
<th>Impact area</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown attack protection</td>
<td>Very good</td>
<td>Unknown applications that try to accept a connection are blocked.</td>
</tr>
<tr>
<td>User restriction</td>
<td>Medium</td>
<td>Users are able to run unknown programs that send traffic to the network, but are not able to run unknown programs that accept connections.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Medium</td>
<td>Only applications that need to be specifically blocked from sending network traffic will have to be added to the specific Programs list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You will need to assign permissions to specific applications that need server rights.</td>
</tr>
</tbody>
</table>

### Phase 3: Block All Non-trusted Communication

These settings are appropriate when you are comfortable that the Trusted Zone is accurately defined and you are not concerned about attacks originating from within your network.

### Impact of Blocking Internet Zone

<table>
<thead>
<tr>
<th>Impact area</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown attack protection</td>
<td>Very good</td>
<td>Unknown applications trying to send traffic or to accept a connection from the Internet Zone are blocked.</td>
</tr>
<tr>
<td>User restriction</td>
<td>High</td>
<td>Users are able to run unknown programs that communicate within the Trusted Zone, but are not able to run those that communicate with the Internet Zone.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Medium</td>
<td>You will need to monitor your programs to ensure your custom program groups are adequate and have the right permissions. You may have to periodically review the Trusted Zone to ensure it is accurate.</td>
</tr>
</tbody>
</table>

### Phase 4: White Listing

This configuration for Unknown Programs prevents applications on the protected computer from communicating with all other computers. This provides the highest possible level of program control, but you must have adequate custom program groups with the correct permission levels to avoid disrupting users.

Remember that this is the setting only for unrecognized programs - other programs are free to connect as needed, according to your definitions of groups and program overrides. Thus, being able to block access to and from Unknown Programs, while maintaining expected performance and connectivity of users, is the goal of this Application Control use case.

### Impact of White Listing

<table>
<thead>
<tr>
<th>Impact area</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown attack protection</td>
<td>Excellent</td>
<td>Unknown applications trying to send traffic or accept a connection are blocked.</td>
</tr>
<tr>
<td>User restriction</td>
<td>High</td>
<td>Users cannot run unknown applications that demand network or Internet access.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>High</td>
<td>You will need to periodically maintain specific program overrides, program group filtering, group permissions, and the Trusted Zone.</td>
</tr>
</tbody>
</table>
Monitoring Applications - Automatic Add

As clients observe new applications running on endpoints, the applications are added to your Application Control list. You can monitor the applications that are added, and you can filter this large list by various criteria.

To monitor controlled applications:
2. Right-click an application group and select Edit Applications.
   The Applications window opens.
   - To view newly observed applications, clear Show only applications which override group permissions and filter for applications observed in the past 24 hours or past week.
     To control whether the new applications are blocked or allowed, double-click the application in the list and set the permissions.
   - To see which applications with permissions that override the group permissions, select Show only programs which override group permissions.
   - To see applications by filename, provide the name (or partial string) in the Look for field. In the Search in field, select File Name. Click Filter.
   - To see applications by file version number, provide the number (or partial string) in the Look for field. In the Search in field, select File Version. Click Filter.

Creating Custom Program Groups

Creating program groups makes it easier to manage program permissions. Program groups allow you to assign permissions to entire groups of programs at once. For example, you can have group permissions for Microsoft Internet Explorer or for Browsers and, depending on its definition, all IE or Browsers will receive the permissions of this group.

As the client observes programs on the endpoint, the programs are added to the appropriate group (according to the criteria you specify) and the permissions you specify for that group are enforced. Thus, you can predefine the permissions for programs before the client observes them requesting network access for the first time.

To create a custom program group:
1. Open Policies > Application Control > Program Groups.
2. Right-click in the Program Groups table where you want to add the new group, and select Add Group.
3. Click either Above or Below, to add the new group to the list in relation to the selected group.
   The Add Program Group window opens.
4. Provide a name and optional comment for the group.
5. If this group should maintain the permissions set here even when clients are disconnected from the Endpoint Security system, select Enable this group in disconnected policies. However, note that this setting is not recommended (to ensure performance).
6. Set the group permissions.
7. In the Program Filter list, click Add.
   The Program Filter window opens.
8. Provide the criteria that determine which programs are added to this group automatically when they are observed running on an endpoint.

Table 17-8 Program Filter Options

<table>
<thead>
<tr>
<th>Program Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publisher</td>
<td>Name of the vendor (for example, Microsoft)</td>
</tr>
</tbody>
</table>
### Changing Group Definitions

Programs are added automatically to groups according to criteria. To remove or add programs to the definition, you need to change or delete the criteria that match the program.

**To change group filters:**
1. Open Policies > Application Control > Program Groups.
2. Double-click the program group.
   - The Program Group window opens.
3. In the Program Filter list, select the filter criteria that match the program you want to remove from this group.
4. Click **Edit**, to tweak the criteria so that it does not match the program; or **Delete**, to remove a specific criteria set from the group definition.

### Deleting Program Groups

If you want to remove a program group, allowing the programs to be added to other groups according to their criteria, you can delete the group definition.

**To remove a program group:**
1. Open Policies > Application Control > Program Groups.
2. Right-click the program group and select **Delete**.

### Managing Unknown Applications

You should check periodically for Unknown Programs. Predefine groups for these programs, to assign permissions to them more efficiently.

**To manage unknown programs:**
1. Open Policies > Application Control > Program Groups.
2. Right-click the Unknown Programs group and select **Edit Programs**.
3. Select the programs to add to a group.
4. Click **Move Program To** and from the drop-down menu, select a group.
5. Confirm the move of the program from Unknown Programs to the selected group.

You can remove programs from groups afterwards.

**To remove programs from groups:**
1. Right-click the group to which you moved the program and select **Edit Group**.
2. Select the filter for the program.
3. Click **Delete** and then **Save**.

---

<table>
<thead>
<tr>
<th>Program Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Name of the program (for example, *.exe). If you want to add a specific program, provide the full name. Partial matches will add any program that matches this name.</td>
</tr>
<tr>
<td>Version</td>
<td>Number of the file. If you want to add programs of a given name but any version, leave this field blank.</td>
</tr>
<tr>
<td>Signed</td>
<td>Select to add only programs that are signed by the vendor; clear to add any programs (signed or unsigned) that match other criteria.</td>
</tr>
</tbody>
</table>
Program Permissions and Disconnected Policies

By default, groups and group permissions exist only on the Endpoint Security Management Server and are not included in the actual policy that is installed on the endpoint. This significantly reduces policy size and improves performance. When the client observes new programs requesting network access, the client asks the server for the permission of the program. The server delivers the permission of the first group to which the program belongs. If a client is unable to contact the Endpoint Security Management Server, the program will receive the permissions you have set for Unknown Programs.

**Important** - Enabling program groups in disconnected policies makes the policies larger (the more groups you add, the bigger the policy becomes) and adversely affects performance, both when connected and when disconnected.

In addition, if more programs are added to a group with this setting, the policy is not updated automatically on the endpoints - you will have to reinstall the policies to the updated program list to the clients.

It is recommended that you use this setting sparingly, only for critical services.

To enable a disconnected policy to control specific program permissions:
1. Open Policies tab > Program Control > Program Groups.
2. Right-click the program group to control when client is disconnected and select Edit Group.
3. Select Enable this group in disconnected policies.
4. Click Save.

Importing Programs

You may wish to identify programs 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.

Use the following features to identify programs by their checksums:

- **Appscans** - You can configure a reference computer with the typical programs on your endpoints. Scanning this computer produces a reference source file that contains all the checksums for all the programs on the computer. You can import this scan file into the Endpoint Security system. This is useful when groups of users have computers with very similar software configurations.

- **Manual Input** - You can also create checksums of individual programs and manually enter them, one by one, into the system. This is only recommended if you have a very limited number of programs to enter.

Scanning Computers

An Appscan is an XML file that contains MD5 and Smart checksums of the programs on a particular computer in your environment.

Using Appscans you can quickly create program rules for the most common applications and operating system files in use on your network. This is especially useful when you have a clean standard image.

Create an Appscan for each disk image used in your environment. You can then create rules that will apply to those applications. You create Appscans 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

Before running the Appscan utility, set up a computer with all the applications that are standard for 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. Copy `appscan.exe` from the tool folder on CD2 to the root directory (typically `c:\`) of the baseline reference source computer.
   To run this utility on Windows 95, 98, or ME operating systems, you also need to copy `unicows.dll`, located in the `<installdir>\checkpoint\Integrity\engine\webapps\ROOT\bin` directory on the Endpoint Security host, to the root directory (typically `c:\`) of the baseline reference source computer.

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

2. On the protected computer, in the command prompt, go to the root directory or to a specific directory to scan (for example, `\program files`).
3. Type `appscan` to begin the scan.
   You can modify the scan through the use of the Appscan switches.
   When the scan is complete, an output file (scan.xml) is created in the directory where you ran the scan.
   Your Appscan file is ready to be imported into Endpoint Security.

**Appscan Switches**

Use the following switches to modify your scan.

*Table 17-9  Appscan Switches and Functions*

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/o</td>
<td>Specifies the output file to be created. If no file name is specified, the default output file name (scan.xml) is used.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> <code>C:\appscan /o scan1.xml [files]</code>&lt;br&gt;In Example 1, the scan is named scan1. The output file name is used when importing it into the Endpoint Security Management Server. If you conduct multiple scans on the same computer, give each scan a unique name.</td>
</tr>
</tbody>
</table>
| /x     | Designates target file names to add to the scan.  
  • The leading period before a file extension is required.  
  • A semi-colon separates the target extensions.  
  • The target extensions are grouped by quotes.  
  • A target directory must be specified using the /s switch.  
  • If the /x switch is not used in the command statement: Only program files (.exe file name extension) are scanned. |
|        | **Example 2:** `C:\appscan /o scan2.xml /x ".exe;.dll" /s "C:\"`<br>In Example 2, the scan is named scan2, and the scan will include .exe and .dll files in the current directory only. |
### Switch | Function
--- | ---
/s | Designates the directory for SmartSum to inventory.  
- If you do not use /s to designate a target directory, the scan will be run in the current directory only.  
- If you use /s, the scan will be run in the target directory and its subdirectories.  

**Example 3:**  
C:\appscan /o scan3.xml /x ".dll" /s c:\program files  
In Example 3, the scan is named scan3. The target directory is C:\program files and all its subdirectories. The target extension is .dll.

**Example 4:**  
C:\appscan /o scan4.xml /x ".exe;.dll" /s c:\program files  
In Example 4, the scan is named scan4. The target directory is c:\program files. The target extensions are .exe and .dll.

/e | Use the /e switch to inventory all executable files in the target directory or drive, regardless of extension.  

**Example 5:**  
c:\appscan /s "C:\program files" /e  
In Example 5, all files are incorporated into the scan.

/a | Generates all file properties for each file inventoried.  

**Example 6:**  
c:\appscan /o scan6.xml /s "C:" /a  
In Example 6, the scan is named scan6. The target directory is the entire contents of c: The output file displays file properties more thoroughly than it would without the /a switch.  
The /a switch does not affect the source.

/p | Displays progress messages.

/verbose | Displays progress and error messages.

/warnings | Displays warning messages.

/ ? or /help | Displays help for Appscan.

## Importing Appscans

After generating an Appscan file, import it into Endpoint Security. You can also import any of the provided Appscans for other versions of Windows from the Samples folder in your installation folder.

> **Note** - You must remove all special characters, such as trademarks, from the appscan before importing it.

### To import an Appscan:

1. Open **Policies > Application Control > Program Groups.**  
2. Click the **Import program list** button on the Program Groups toolbar.  
The **Import Programs** window opens.
3. Browse to the Appscan file: **scan.xml**
4. Click **Import.**  
When applications listed in this file are observed on endpoints, they are added to the Referenced Programs group and the properties from your reference computer overwrite observed properties.
Manually Adding Programs

You can predefine program control for applications before they are observed. You can also use this procedure to ensure that a specific program is treated differently than the program group to which it would otherwise belong.

To manually add a program to controlled programs:
1. Open Policies > Application Control > Program Groups.
2. Click the Add program manually button on the Program Groups toolbar.
   The Add Program Manually window opens.
3. Enter the MD5 Checksum
4. Enter the Smart Checksum, if this program is in a scan.xml file created from an Appscan.
5. Provide as many of the details of the program as possible:
   - File Name, Product Name
   - File Version, Product Version
   - Publisher (vendor)
   - Language

Program Advisor

Check Point IPS Program Advisor provides Application Control recommendations. Use Program Advisor to get professional recommendations from Check Point security professionals about which permissions to assign to common programs. This reduces your workload while improving security and usability.

Program Advisor also includes a significant list of known malicious programs. These are grouped in the PA Terminated Programs group, which is always the first program group in the Programs list, and therefore always has precedence: any known malicious program attempting to access your network or the Internet as either client or server will be blocked and then the program will be terminated.

*Note* - Program Advisor requires that Endpoint Security have Internet access (on ports 80 and 443) to connect to the Check Point Program Advisor Server: ensure that your firewall allows this traffic. It is also recommended that you add the Program Advisor Server to your Trusted Zone.

Program Advisor Server

The Program Advisor Server contains a database of program permissions that is constantly updated by Check Point security professionals. It provides program permissions to the Endpoint Security Management Server. These permissions are accepted by default, but you override them with custom recommendations of your own.

Viewing Program Advisor Recommendations

Program Advisor displays recommendations for programs when the programs are observed on the endpoint computer.

To view the Program Advisor recommendations:
1. Open Policies > Application Control > Program Groups.
2. Right-click PA referenced programs and select Edit Programs.
   or
   Right-click PA terminated programs and select Edit Programs.

*Note* - If there is a long delay between a client asking Program Advisor about a program and the log upload containing the observation for that program, and if there is also a Program Advisor recommendation for that program, the program recommendations may appear incomplete.
Using Program Advisor with a Proxy Server

If your environment includes a proxy server for Internet access, perform the configuration steps below to let the Endpoint Security Management Server connect to the Check Point Program Advisor Server through the proxy server. Note that all configuration entries are case-sensitive.

To configure a proxy server in Windows:

2. Open:
   
   C:\Program Files\CheckPoint\CPuepm\80.20\engine\conf\local.properties
3. Add these properties:
   
   a) Specify the proxy server's IP address as shown in the example below:
      
      http.proxy.host=123.456.78.90
   
   b) Specify the proxy server's listening port as shown in the example below:
      
      http.proxy.port=8080
   
   c) Specify the username if basic authentication is enabled on the proxy server. Leave it empty if no authentication is required.
      
      http.proxy.user=<username>
   
   d) Specify the password if basic authentication is enabled on the proxy server.
      
      http.proxy.password=<password>
4. Save the local.properties file.
Chapter 18

Endpoint Compliance

The Endpoint Compliance blade makes sure that:

- All required Endpoint Security packages, with version updates, are installed on the endpoint computer.
- Required operating systems, with versions, service packs, and updates are installed on the endpoint computer.
- Only authorized programs are installed and running on the endpoint computer.
- Configured Registry keys and values are present.

You can configure Endpoint Security to assign restrictive firewall, Access Zones, Application Control, and Media Encryption & Port Protection policies to endpoint computers that do not match compliance policy rules. These restrictive policies can block endpoint computer access to some or all network resources.

You can use SmartView Tracker to see logs that show endpoint compliance and remediation actions.

In This Chapter

- Compliance Status 143
- Quick Start 144
- Planning Compliance Rules 144
- Creating a Endpoint Compliance Policy 144
- Viewing Endpoint Compliance Policy Assignments 145
- Endpoint Compliance Policy 145
- Endpoint Compliance Assignment 146
- Check Object 147

Compliance Status

The Compliance Status area on the Overview tab shows the percentage of endpoint computers for each compliance category.

To show compliance status by organization:
1. From the Monitor area on the Overview tab, select the Compliance Status report.
2. Click the My Organization browse button to select the scope of the report.
   - The report can cover all the organization, a directory, network, group, user, or one endpoint computer.
   - The pie chart shows the percentage of endpoint computers that match the predefined compliance categories.

To show compliance status by user:
1. Click Show Details.
2. From Filter, select User Name or Computer Name.
3. From Statuses, select All or one of the status categories.
4. The compliance status of individual users is shown in the table.

Note - Click Export to File to copy the compliance status information shown in the table to Excel or CSV.
Quick Start

This section explains how to quickly assign predefined Endpoint Compliance policies.

These Endpoint Compliance policies are available:

- **High Security Compliance Level** - Recommended consistent endpoint security, functionality and maintenance in a large environment.
- **Medium Security Compliance Level** - Recommended for consistent endpoint security and maintenance. Users can install and use worked-related applications.
- **Low Security Compliance Level** - Recommended for control of endpoint security, without required operating system update level or application control.

**To assign a policy:**
1. On the Endpoint Security Management Server console, click the **Policies** tab and select **Endpoint Compliance Policies** on the **Navigation** tree.
   The **Endpoint Compliance Overview** page opens.
2. Double-click one of the predefined policies.
   The **Endpoint Compliance Policy** window opens.
3. Click **Assignment**.
   On the **Assignment** window, click **Add Assignment** and select from the **Navigation** tree. Click **OK**.
   The assignment is shown on the **Assignment** ("Endpoint Compliance Assignment" on page 146) window.
4. Click **OK**.

Planning Compliance Rules

Before creating compliance rules:

1. Identify the applications, files, registry keys, and process names to be allowed or disallowed on the endpoint computers.
2. Configure rules the endpoint computer must comply with, and what to do if the endpoint fails to comply. Start by using rules that **Observe** or **Warn** users as an alternative to restricting them. Later, configure rules to restrict non-compliant users.
3. Collect all information and resource files necessary for user compliance. Refer to this information when you specify remediation resources in the compliance rules.
   Compliance rules can prevent users from accessing the required network resources when they are out of compliance. Make it easy for users to become compliant.
4. Make sure that the firewall polices gives access to remediation resources. For example, sites from which service packs or Anti-virus updates can be downloaded.
   **Note** - In Windows 7, make the Interactive Service Detection service is running. This is necessary for remediation files (running with system credentials) that need to interact with the user.
5. Set compliance rule alerts and logon policies to enforce the rules after deployment.
6. Pay attention to the interval between one compliance check and the next. Set a reasonable value in the Endpoint Security Management Console.

Creating a Endpoint Compliance Policy

This section explains how to create an Endpoint Compliance policy.

**To create a compliance rules policy:**
1. In the Endpoint Security Management Console, open the **Policies** tab.
2. In the **Navigation** tree, select **Compliance Rules**.
   The **Compliance Rules Overview** page opens.
3. From View By, select Policies.
4. Click New.
5. The Endpoint Compliance Policy window opens.
6. Configure the compliance settings.
7. Click OK.
8. Click Save & Install.

Viewing Endpoint Compliance Policy Assignments

Policies can be assigned to all of the organization, networks, directories, groups, and users. Multiple policies can be assigned to the user and endpoint computer.

To show policy assignments:
1. On the Policy tab > click Compliance Rules in the navigation tree.
2. From the View By drop-down box, Select Assignments.

Endpoint Compliance Policy

This section explains how to configure Endpoint Compliance for Endpoint Security packages, operating system service packs, and application control.

Before configuring a compliance policy:
1. Open the Endpoint Security Management Console
2. Open Manage > General Properties and configure these settings:
   - Connection Settings (“Configuring the Heartbeat Interval” on page 63)
     Make sure to set:
     - An interval between heartbeats
     - For how many heartbeats the endpoint can be out of compliance (5 by default)
   - Authentication Settings (“Endpoint Security Active Directory Authentication” on page 44)

General Configuration

To Configure a Compliance Policy:
1. In the Endpoint Security Management Console, click the Policies tab.
2. On the navigation tree, click Compliance Rules.
3. From the View By drop-down box, select Policies.
4. Double-click an existing policy or create a new one. The Compliance Rules Policy window opens.
5. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security Client</td>
<td>Monitors the client’s version. Click Manage to add or remove a Deployment Profile Check object. The Client Profile Check object makes sure that the Endpoint Security package specified in the profile is installed on the user’s computer.</td>
</tr>
<tr>
<td>OS Service Packs and Updates</td>
<td>Checks operating system service packs and updates. Click Manage to add or remove a Security Pack Check object. A Security Pack Check object identifies the operating system registry key and value.</td>
</tr>
</tbody>
</table>
## Prohibited Applications and Files
Checks for forbidden applications.
Click **Manage** to add or remove an Application Compliance Check object. An Application Compliance Check object is used to identify the presence of:
- An application registry key and value
- A file name and its properties
- An application that it is running

## Required Applications & Files
Checks for required applications.
Click **Manage** to add or remove an Application Check object. An Application Check object is used to identify:
- An application registry key and value
- A file name and value
- An application that is not running

## Anti-Virus
Checks for Anti-Virus program
Click **Manage** to add or remove an Anti-Virus Check object. An Anti-Virus Check object is used to identify:
- An Anti-Virus Provider
- Minimum engine version
- DAT file updates

Apply one of these actions to an endpoint computer in violation of the compliance policy:

<table>
<thead>
<tr>
<th>Action</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Observe</strong></td>
<td>Log endpoint activity. The user is not aware of being non-compliant.</td>
</tr>
<tr>
<td><strong>Warn</strong></td>
<td>Alert the user about non-compliance and provide remediation resources</td>
</tr>
<tr>
<td><strong>Restrict</strong></td>
<td>Alert the user about non-compliance and provide remediation resources</td>
</tr>
<tr>
<td></td>
<td>Log to the administrator</td>
</tr>
<tr>
<td></td>
<td>Change relevant polices to the restricted type after a pre-defined number of heartbeats. Before that happens, the user is in the <em>about to be restricted</em> state. On the monitoring tab, the user is shown as <em>pre-restricted</em>.</td>
</tr>
</tbody>
</table>

**Note** - With **Restrict** or **Warn**, you can select a remediation object, which runs an executable file that corrects the problem.

Clients move to the **About to be Restricted** state if the **Action** of a compliance rule is **Restricted** but the **Out of Compliance** period did not pass.

## Custom Rules
Custom rules can also be used to configure an Endpoint Compliance policy. Compliance values selected in **General Properties** for Endpoint Security packs, operating system service packs, and application controls are displayed here.

**Custom Rules** let you identify rules by a unique rule name. Use the **Custom Rule** buttons to set the sequence in which messages show on the endpoint after a compliance violation.

## Endpoint Compliance Assignment
For compliance to work, Endpoint Compliance policy must be assigned to:
- A user
- An endpoint computer or group of endpoint computers.

If assigned to a computer, all users of that computer receive the same policy. If assigned to a user, the policy is unique to that user.

**To assign a policy:**
1. In the **Policies** tab, in the **Overview** page of a blade, open an existing policy or create a new one.
2. The **Policy** window opens.
3. Click **Assignment** in the navigation tree.
4. Click **Add Assignment**.
   The **Select Node** window opens.
5. In the **Navigation Tree**, select a node in the directory. When you select a directory or group, users that belong to that group or directory show in the **Node** area.
6. Click **OK**.
7. On the **Assignment** page, click the **Add Assignment** down arrow, and select from the displayed options.
8. Click **OK**.
9. Click **Install Policies**.

**To assign a different policy:**
1. On the **Assignment** page, select the node row and click the **Assign Different Policy** down arrow.
   The list of policies is shown.
2. Select a policy.
3. Click **OK**.
4. Click **OK**.
5. Click **Install Policies**.

---

**Check Object**

A check object is used to identify a client profile, application files, or keys in the Windows registry of an endpoint computer. Show check objects by clicking the **Checks** tab on the **Custom Rules** page.

The check object types are:

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom check</td>
<td>Monitors registry keys, values, and applications</td>
</tr>
<tr>
<td>Group check</td>
<td>Groups multiple check objects</td>
</tr>
<tr>
<td>Application Compliance check</td>
<td>Monitors applications and registry keys</td>
</tr>
<tr>
<td>Client Profile check</td>
<td>Identifies the endpoint computer profile to install Endpoint Security packs</td>
</tr>
<tr>
<td>Service Pack check</td>
<td>Identifies service pack properties.</td>
</tr>
</tbody>
</table>

**To create a check object:**
1. In the **Custom Rules** window, open the **Checks** tab.
2. Click **New**.
   The **Select New Object** window opens.
3. Select a check object type.
4. Click **OK**.
5. The check's properties window opens.
6. Enter the check object details
7. Click **OK**.
Check Object

Custom Check and Application Compliance Check Properties

A Custom Check object can be used to make sure that:

- Required executable files are present and running on the endpoint
- Prohibited executables are not present or running on the endpoint

When creating or editing a Custom Check or Application Compliance Check object, enter these details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Registry</td>
<td>Select either:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Registry key and value exist</strong> - Find the registry key and value.</td>
</tr>
<tr>
<td></td>
<td>If the file exists, the endpoint computer is compliant for the required</td>
</tr>
<tr>
<td></td>
<td>file.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Registry key and value do not exist</strong> - Make sure the registry key and</td>
</tr>
<tr>
<td></td>
<td>value does not exist.</td>
</tr>
<tr>
<td></td>
<td>If the key does not exist, the endpoint computer is compliant for an</td>
</tr>
<tr>
<td></td>
<td>application that is prohibited.</td>
</tr>
<tr>
<td>Registry Key</td>
<td>Enter the registry key to identify.</td>
</tr>
<tr>
<td>Registry Value</td>
<td>Enter the registry value that matches the Check Registry type.</td>
</tr>
<tr>
<td>Check File</td>
<td>Select one of these to check if an application is running or if a file exists:</td>
</tr>
<tr>
<td></td>
<td>- <strong>File is running at all times</strong> - For example, make sure that Endpoint</td>
</tr>
<tr>
<td></td>
<td>Security client is always running.</td>
</tr>
<tr>
<td></td>
<td>- <strong>File exists</strong> - For example, make sure that the user browsing history</td>
</tr>
<tr>
<td></td>
<td>is always kept.</td>
</tr>
<tr>
<td></td>
<td>- <strong>File is not running</strong> - For example, make sure that DivX is not used.</td>
</tr>
<tr>
<td></td>
<td>- <strong>File does not exist</strong> - For example, make sure that a faulty dll file</td>
</tr>
<tr>
<td></td>
<td>is removed.</td>
</tr>
<tr>
<td>File Name</td>
<td>Enter the name of the file to find. It can be any file, but if we want the</td>
</tr>
<tr>
<td></td>
<td>file to run or not run, you must enter the name of the process. (either</td>
</tr>
<tr>
<td></td>
<td>.exe or .bat)</td>
</tr>
<tr>
<td>File Path</td>
<td>• Enter the path, but do not include the file name.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Use environment Variables of logged in user</strong> attribute includes</td>
</tr>
<tr>
<td></td>
<td>paths defined in the endpoint computer's system and user variables.</td>
</tr>
<tr>
<td>Check File Properties</td>
<td>Additional options to check for an existing or non-existing file.</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 MD5 Checksum. Click <strong>Calculate</strong> to compare the checksum</td>
</tr>
<tr>
<td></td>
<td>on the endpoint with the checksum on the server.</td>
</tr>
<tr>
<td>File is not older than</td>
<td>Find the file by the number of days on the endpoint computer.</td>
</tr>
</tbody>
</table>

Remediation Objects and Client Remediation Messages

A Remediation object runs an application or file to make the endpoint computer compliant. To see the list of Remediation objects, open **Custom Rules > Remediations** tab.

**To create a Remediation object:**

1. On the **Remediations** tab, click **New**.
   - The **Run File Remediation Properties** window opens.
2. Configure these **Operation** and **Message** options:

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
<td></td>
</tr>
<tr>
<td>Run Custom File</td>
<td>Activates the <strong>Run Custom File</strong> option.</td>
</tr>
</tbody>
</table>
| Download Path                                  | - The Download Path is a temporary directory on the local computer to which the file should be downloaded. This path must be a full path that includes the actual file with one of the supported extensions (*.bat or *.exe).
   - The path cannot be empty.
   - The endpoint client first tries to access the file from the specified path. If the client fails, it downloads the file from the URL to the temporary directory and runs it from there.
   - To run multiple files, use one of the popular compression programs such as WinRar to produce a self-extracting executable that contains a number of .exe or .bat files. |
| URL                                            | - Enter the URL of an http 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 path 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. |
| Run as System                                  | Apply system rights for running the executable file. Not all processes can run with user rights. System rights may be required to repair registry problems and uninstall certain programs. |
| Run as User                                    | Apply user rights and local environment variables for running the executable file. |
| **Messages**                                   |                                                                                  |
| Automatically execute operation without user notification | Run the executable file without displaying a message on the endpoint computer. |
| Execute operation only after user notification | Run the executable file only after asking approval. |
| Use same message for both Non-Compliant and Restricted messages | Select that the same text be used for both messages.
   - A Non-Compliant message tells the user that the endpoint computer is non-compliant and provides details of how to achieve compliancy.
   - A Restricted message tells the user that the endpoint computer is non-compliant, provides details of how to achieve compliancy, and restricts computer use until compliancy is achieved. |
Message Box | Displays selected non-compliant and restricted messages. The message box is available only by selecting the Execute only after user notification setting. Click Add, Remove, or Edit to add a message, and remove or revise a selected message.

Note: User cannot prevent the remediation application or file from running.

Client Message Properties

When Warning or Restricted is the selected action on a compliance check, such as Prohibited Applications & Files, a message shows on the client.

To create a client text message:

1. Open the Compliance Rule Policy > General Properties page.
2. For a specified compliance check, click Manage.
   The Run File Remediation Properties window opens.
3. In the Messages area, click Add.
   The New Client Message Properties window.
4. From the Locale drop down box, select a language for the message.
5. From the Non-compliant Message or Restrict Message drop-down box:
   - Select an existing message or
   - Click Manage to create a new one.
   The Client Messages Properties window opens.
6. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Select the language.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the message title.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the message text.</td>
</tr>
<tr>
<td>Confirmation Text</td>
<td>The text displayed in the message for the user to click as confirmation.</td>
</tr>
</tbody>
</table>

7. Click OK.
   The new client message shows in the Remediation Message box.

Group Check Properties

A Group Check object is a container that holds multiple check objects (application checks, service pack checks, custom checks).

To create a Group Check object:

1. On the Policies tab > Compliance Rules page, open an existing policy (or create a new one).
   The Compliance Rules Policy window opens.
   The Select New Object Type window opens.
3. From the list, select Group Check.
   The Group Check Properties window opens.
4. Configure the endpoint to satisfy all the checks in the list, or only one of them.
5. Click Add > New to create more check objects.

Client Profile Check Properties

The Client Profile Check object identifies Endpoint Security endpoint computers for update purposes.

To create a client profile check:

1. On the Policies tab > Compliance Rules page, open an existing policy (or create a new one).
The **Compliance Rules Policy** window opens.

2. On the **Custom Rules** page > **Checks** tab, click **New**. The **Select New Object Type** window opens.

3. From the list, select **Client Profile Check**.

4. The **Client Profile Check Properties** Window opens.

5. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Select the deployment profile. The profile identifies the endpoint package version.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the Windows version.</td>
</tr>
</tbody>
</table>

### Service Pack Check Properties

A Service Pack Check object identifies Window operating system files on the endpoint computer that must be updated.

**To create a Service Pack check:**

1. On the **Policies** tab > **Compliance Rules** page, open an existing policy (or create a new one). The **Compliance Rules Policy** window opens.

2. On the **Custom Rules** page > **Checks** tab, click **New**. The **Select New Object Type** window opens.

3. From the list, select **Service Pack Check**.

4. The **Service Pack Check Properties** Window opens.

5. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Select the Windows version</td>
</tr>
<tr>
<td>Registry Key</td>
<td>Enter the registry key for the service pack.</td>
</tr>
<tr>
<td>Registry Value</td>
<td>Enter the registry value for the service pack.</td>
</tr>
</tbody>
</table>
WebCheck protects the endpoint computer against phishing - websites impersonating other websites for malicious purposes. WebCheck creates a virtual browser with its own virtual file system. It opens any site that is not defined as trusted in the virtual browser. Any changes made by a non-trusted site, for example the introduction of malware, are confined to the virtual browser file system.

- See the Release Notes for supported browsers.

### Enabling WebCheck

To enable WebCheck:

1. Open the Endpoint Security Management Console.
2. On the Policies tab, select WebCheck.
4. On the General Properties page, select Enable WebCheck. This adds WebCheck to the policy.
5. Select WebCheck options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Site Status Check</td>
<td>Rates security level of each site visited. WebCheck displays a warning message when users visit a suspicious site. The user can click the Read More link in the message to see more information about the site.</td>
</tr>
<tr>
<td>Enable Site Visits Log</td>
<td>Logs all URLs that the user visits.</td>
</tr>
<tr>
<td>Enable Anti-phishing (signature)</td>
<td>Tracks recently discovered phishing and spyware sites, and interrupts browsing with a warning message.</td>
</tr>
<tr>
<td>Enable Anti-phishing (Heuristics)</td>
<td>Examines sites for phishing characteristics.</td>
</tr>
<tr>
<td>WebCheck trusted sites</td>
<td>Creates lists of sites (&quot;Creating Trusted Sites&quot; on page 152) that are safe to exclude from WebCheck.</td>
</tr>
</tbody>
</table>

### Creating Trusted Sites

A trusted site is a site for which WebCheck is not required. For example a site within the corporate network would be considered safe and therefore trusted. With the trusted sites option, WebCheck creates different browsing environments:

- One for trusted sites within the corporate zone.
• One for the non-trusted Internet zone.

Trusted sites are opened directly in the end-user's browser. Non-trusted sites are opened in the WebCheck virtual browser.

To Create a Trusted Site or Group of Sites:
1. Open the Endpoint Security Management Console.
2. On the Policies tab, select WebCheck.
   The WebCheck Policy window opens.
   This adds WebCheck to the policy.
5. Click WebCheck trusted sites.
6. Click Add, and select Site Pattern Properties.
7. In the Site Pattern Properties window, enter:
   a) A descriptive name in the Name field.
   b) A Host Name according to one of the permitted formats:

```
<table>
<thead>
<tr>
<th>Permitted Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>company.com</td>
<td>Domain name for a single host</td>
</tr>
<tr>
<td><a href="http://www.company.com">www.company.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.*.company.com">www.*.company.com</a></td>
<td>Domain with wild card for sub-domain</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>IP address for a single host</td>
</tr>
</tbody>
</table>
```

   Note - URLs are not permitted.

8. Click Add > New > Site Pattern Group to collect single sites into an easily managed group.

Temporarily Disabling WebCheck

In rare cases, WebCheck can interfere with normal browsing. To resolve these issues, Check Point supplies a utility (NOISW.exe), that lets users temporarily disable WebCheck protection. This utility is not documented in the Endpoint Security User Guide. We recommend that you do not tell users about NOISW.exe, unless there are no alternatives that resolve the issue.

When a user runs NOISW.exe, WebCheck is disabled for a user-defined period of time. An alert appears in the WebCheck Status pane on the Monitoring tab.

To let a user temporarily disable WebCheck, give these instructions:
1. Close all Web browsers.
2. Run NOISW.exe, located in the Program Files\CheckPoint\Endpoint Security\WebCheck folder.
3. Enter the number of minutes to disable WebCheck. The default is 15 minutes.
4. In the WebCheck window, click Suspend.
5. Click OK to confirm.
Chapter 20

Common Client Settings

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

A Common Client Settings policy is a policy shared by a number of endpoints, these endpoints being Organizational Units in the Active directory, Virtual Directory Structure, or single computers. A common policy is created in the Common Client Settings Overview window.

Common Client Settings Properties

In the Common Client Settings Policy page, you can:

- View how current policies are assigned
- Create new policies
- Edit current policies
- Add or remove policies

The Common Client Settings policy sets:

- 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

Setting a Common Client Policy

To set a Common Client Settings Policy:

1. Open the Endpoint Security Management Console.
2. On the Policies tab, select Common Client Settings.
   
   The Common Client Settings Policy Overview page shows.
3. Click New.
   
   The Common Client Settings Policy window opens.
4. On the General Properties page, configure these options:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Properties</td>
<td>Name</td>
<td>A descriptive name for the policy</td>
</tr>
</tbody>
</table>

In This Chapter

Common Client Settings Properties 154
Setting a Common Client Policy 154
### Setting a Common Client Policy

#### Common Client Settings

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Notification Area Settings</td>
<td>Display client icon</td>
<td>Select to show the client icon in the windows notification area when the Endpoint Security client is installed.</td>
</tr>
<tr>
<td>Client Install / Uninstall Settings</td>
<td>Enable the user to postpone the client installation or upgrade.</td>
<td>When users get a message that the installation is ready, let them choose to postpone the installation.</td>
</tr>
<tr>
<td></td>
<td>• Remind the user to install new client every</td>
<td>• Set the time, in minutes, after which users are reminded to install the client.</td>
</tr>
<tr>
<td></td>
<td>• Force installation and automatically restart after</td>
<td>• Set the time, in hours, after which the installation starts automatically.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client Uninstall Password</td>
<td>Set a password that the end user must enter before uninstalling the client.</td>
</tr>
<tr>
<td></td>
<td>Legacy Client Uninstall Password</td>
<td>Passwords that the end user must enter before uninstalling a legacy client</td>
</tr>
<tr>
<td>Log Upload Settings</td>
<td>• Log Upload interval</td>
<td>Conditions that must be met before logs are uploaded to the server. These policies upload logs to the Endpoint Security Management Server:</td>
</tr>
<tr>
<td></td>
<td>• Minimum number of events before attempting an upload</td>
<td>• Desktop Firewall</td>
</tr>
<tr>
<td></td>
<td>• Maximum number of events to upload</td>
<td>• Application Control</td>
</tr>
<tr>
<td></td>
<td>• Maximum age of event before upload</td>
<td>• Malware Protection, compliance)</td>
</tr>
<tr>
<td></td>
<td>• Discard event if older than</td>
<td>• Full Disk Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WebCheck</td>
</tr>
<tr>
<td>Network Protection Settings</td>
<td>Allow network protection shutdown</td>
<td>Lets the user shut down network protection by right-clicking the icon in the Notification Tray and selecting the shutdown option.</td>
</tr>
<tr>
<td></td>
<td>Network Protection Alerts</td>
<td>Alerts are client-side pop-up messages. This setting determines whether clients get alerts and whether alerts generate logs.</td>
</tr>
</tbody>
</table>

1. In the navigation tree, select **Assignment**.
2. The **Assignment** page shows.
3. Click the downward pointing arrow on the **Add Assignment** button to specify an Assignment state for the Common Client Policy.
   The assignment states are:
   - Connected to Enterprise
   - Disconnected from Enterprise
   - Restricted
   The policy is applied when the client is in the specified state.
   Once a state is assigned, the **Select Node** window opens.
4. In the **Select Node** window, select a node or nodes from the **My Organization** tree.
   **Note** - An existing assignment can be removed, or a different policy assigned.
5. Click **OK**.
6. Select **File > Save**.
Chapter 21
Remote Help

Overview of Remote Help

Users can be denied access to their Full Disk Encryption-protected endpoint computers or Media Encryption & Port Protection-protected devices for a number of reasons. For example, they might have entered an incorrect password too many times or forgotten their password or, in a worst case scenario, a hacker might have tried to break into their computer or device.

Remote Help is designed to assist users in these types of situations. The user calls the designated Endpoint Security administrator and follows the Remote Help procedure.

Note - An Endpoint Security administrator can provide Remote Help to users who have been denied access to their Full Disk Encryption protected computers, or computers with Media Encryption & Port Protection only if you enabled Remote Help in the OneCheck User Settings policy.

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 USB storage devices protected by Media Encryption & Port Protection policies, only remote password change is available.

Process for Remote Help

This section covers the Remote Help workflow for Full Disk Encryption and Media Encryption & Port Protection:

1. The user is locked out of the endpoint computer or the device and calls the Endpoint Security administrator for assistance.
2. The Endpoint Security administrator verifies that the person requesting Remote Help is an authorized user of the computer or device before providing assistance.
3. After the identity of the user has been verified, the user and Endpoint Security administrator perform the Remote Help challenge/response procedure.
4. The system or device is unlocked and the user has access.
Providing Full Disk Encryption Remote Help

To provide Full Disk Encryption Remote Help assistance:
   The User Logon Preboot Remote Help window opens.
2. Select the type of assistance the end-user needs:
   a) One Time Login. One Time Login allows 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 who needs Remote Help.
4. In the Device Name field, use the drop-down list to select the endpoint computer assigned to the user that needs Remote Help.
   Note - Alternatively, you can click the My Organization tab and right-click a user from the Users folder. Select User Logon Preboot Remote Help. The User Logon Preboot Remote Help window opens with the user name and device name filled in.
5. Click Generate Response.
6. Tell the user to enter the Response One on the Client into the Remote Help window on the locked computer.
   The user receives a challenge code.
7. In the Challenge From User field, enter the challenge code 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 Response Two on the client into the Remote Help window on the locked computer.
10. Make sure that the user changes the password or gains one-time access to the computer successfully before ending the Remote Help session.

Providing Media Encryption & Port Protection Remote Help

Media Encryption & Port Protection lets administrators recover removable media passwords remotely using a challenge/response procedure. Always verify that the person requesting Remote Help is an authorized user of the removable media before providing assistance.

To recover a Media Encryption & Port Protection password:
   The Media Encryption & Port Protection Remote Help window opens.
2. In the User Logon Name field, click the browse button and select a user to whom you want to provide Remote Help.
   Note - Alternatively, you can click the My Organization tab and right-click a user from the Users folder. Select Media Encryption & Port Protection Remote Help. The Media Encryption & Port Protection Remote Help window opens with the user name filled in.
3. In the Challenge From User field, enter the challenge code the user gives you.
4. Click Generate Response.
   Media Encryption & Port Protection authenticates the challenge code and generates a response code.
5. Provide the response code to the user.
6. Ensure that the user is able to access the 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.
Index

A
About Policies • 59
Access to Media Encryption & Port Protection Policies • 103
Access Zones Policies • 117
Account Lockout • 83
Active Directory Scanner • 23
Active versus Standby • 71
Activity Reports • 55
Adding Network Objects • 118
Advanced Media Log • 108
Advanced Settings • 116
Anti-Malware • 56
Application Control Policies • 129
Appscan Switches • 139
Assigning Policies • 63

B
Backup and Restore • 80

C
Centralized Deployment • 13
Centralized Monitoring • 13
Centralized Organization of Users and Computers • 13
Changing a Server to Active or Standby • 71
Changing a User's Password • 67
Changing an Existing Access Zones Policy • 121
Changing Group Definitions • 137
Changing the Clean Up Task Status • 18
Changing the Group Ranking Order • 111
Check Object • 147
Client logging • 42
Client Packages on the Installation CD • 37
Client Profile Check Properties • 150
Client Requirements for Full Disk Encryption Deployment • 95
Common Client Settings • 154
Common Client Settings Properties • 154
Completing Full Disk Encryption Deployment on a Client • 96
Compliance • 55
Compliance Status • 143
Configuring a Client Package with a Default VPN Site • 38
Configuring a Directory Scanner Instance • 24
Configuring a Group as a Network Object • 120
Configuring a Host as a Network Object • 119
Configuring a Network as a Network Object • 119
Configuring a Network Group With Exclusion • 120
Configuring a Site as a Network Object • 119
Configuring a Site Group as a Network Object • 120
Configuring Active Directory for Authentication • 45
Configuring an Address Range as a Network Object • 119
Configuring Authentication • 45
Configuring Authentication Settings • 46
Configuring Log Forwarding • 78
Configuring Media Encryption Sites • 110
Configuring OneCheck User Settings • 83
Configuring Policy Enforcement • 61
Configuring Policy Server Settings • 76
Configuring Software Signatures • 38
Configuring the • 62
Configuring the Apache Cache • 18
Configuring the Directory Scanner for the First Time • 24
Configuring the Heartbeat Interval • 63
Configuring the Proximity Analysis Interval • 77
Configuring VPN Client Settings • 40
Converting Legacy Encrypted Devices to Media Encryption • 111
Creating a Basic Package • 36
Creating a Customized Full Disk Encryption Policy • 88
Creating a Endpoint Compliance Policy • 144
Creating a Malware Protection Policy • 124
Creating an Appscan • 138
Creating Application Control Configuration • 129
Creating Custom Media Authorization Settings • 107
Creating Custom Program Groups • 136
Creating Data Recovery Media • 97
Creating Exceptions to Device Logging • 108
Creating Firewall Rules • 115
Creating New Access Zones Definitions • 121
Creating Rules for Non-Encrypted Devices • 105
Creating Trusted Sites • 152
Custom • 57
Custom Check and Application Compliance Check Properties • 148
Custom Rules • 146
Custom Scan Level Settings • 126

D
Deleting Program Groups • 137
Demo and Product Licenses • 31
Deploying Endpoint Security Clients • 34
Deploying Policies • 66
Deployment Overview • 34
Direct Assignment • 63
Directory Synchronization • 26
Disabling Remote Help • 158
Disabling the Preboot Temporarily • 67
Distributing by Exporting the Package • 40
Distributing Software Blade Packages and Updates • 39
Distributing the Initial Client • 35
Distributing with Assignments • 39
Drive Encryption • 88
Dynamic Mount Utility • 102

E
Editing Program Group Permissions • 131
Editing Specific Program Permissions • 132
Enabling or Disabling a Scanner Instance • 26
Enabling the Management Server to be a Policy Server • 77
Enabling WebCheck • 152
Encrypting Removable Media • 106
Endpoint Compliance • 143
Endpoint Compliance Assignment • 146
Endpoint Compliance Policy • 145
Endpoint Policy Server Proximity Analysis • 77
Endpoint Security Active Directory Authentication • 44
Endpoint Security Administrator Roles • 27
Endpoint Security License Types • 31
Endpoint Security Licenses • 31
Endpoint Security Services and Ports • 12
Enforcing Policies According to States • 61
Evaluation Mode Client • 43
Example 1 • 114
Example 2 • 114
Examples of Rule Numbers • 114
Exceptions for Specified Non-Encrypted Devices • 105
External Endpoint Policy Servers • 76
Finding Components in the Console • 58
Firewall Rule Number • 114
Firewall Rules - Control Icons and Buttons • 112
Firewall Rules Policies • 112
Firewall Rules Policy Options • 112
Full Access Role • 28
Full Disk Encryption • 57
Full Disk Encryption Deployment Phase • 101
Full Disk Encryption Installation and Deployment • 95
Full Disk Encryption Logs • 101
Full Disk Encryption Policies • 87
Full Disk Encryption Recovery • 97
Full Disk Encryption Troubleshooting • 99
General Configuration • 145
General Properties • 104
Getting and Applying Contracts • 32
Getting Licenses • 32
Getting the Initial Client from the Console • 35
Global Package Configurations and Content • 38
Global Settings on the Overview Page • 103
Group Assignment Priority • 64
Group Check Properties • 150
Help Desk Role • 29
High Availability Deployment Considerations • 71
How Application Control Functions • 132
How do Endpoint Policy Servers Work? • 76
How to Back Up and Restore • 80
Important Information • 2
Importing Appscans • 140
Importing Programs • 138
Inherited Assignment • 64
Installing a Server for High Availability • 21
Installing Endpoint Security Management Console • 19
Installing Endpoint Security Servers • 14
Installing External Endpoint Policy Servers • 19
Installing the Client Using the CLI • 41
Installing the Endpoint Security Management Server • 16
License Behavior • 32
License Status • 33
Licenses Status Report • 58
Malware Protection - Assignment Settings • 128
Malware Protection - Engine & Signature Updates • 127
Malware Protection - Scan Exclusion and Processes • 127
Malware Protection - Settings • 124
Malware Protection Policies • 123
Malware Protection Settings • 125
Management High Availability • 70
Management Server Configuration in the Configuration Tool • 17
Management Server Configuration in the Console • 17
Managing Computers • 68
Managing Networks • 54
Managing OUs or Groups • 67
Managing Policies and Users • 59
Managing Unknown Applications • 137
Managing Users • 66
Managing Users of a Computer • 68
Manually Adding Programs • 140
Media Encryption & Port Protection • 57
Media Encryption & Port Protection Policies • 103
Media Encryption & Port Protection Terminology • 103
Media Encryption & Port Protection User Alerts • 109
Media Encryption Sites • 109
Monitoring Applications - Automatic Add • 135
Monitoring Endpoint Policy Server Activity • 79
Monitoring Tab • 55
My Organization Tab • 53
Network Objects • 118
Non-Compliance • 61
Offline Upgrades • 50
OneCheck Logon • 94
OneCheck User Settings Assignments • 83
OneCheck User Settings Permissions • 85
OneCheck User Settings Policies • 82
Online Upgrades • 51
Optional System Components • 11
Organization-Centric model • 13
Overview of Backup and Restore • 80