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=12649)
To learn more, 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>03 November 2013</td>
<td>Updated links to the E80.30 homepage to sk65921. Added clarification in Malware Signatures and Engine Updates (on page 151). Improved formatting and document layout.</td>
</tr>
<tr>
<td>6 December 2011</td>
<td>In How to Back Up and Restore (on page 92), changed Migrate.exe to migrate.exe.</td>
</tr>
<tr>
<td>9 November 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 E80.30 Administration Guide).
Contents

Important Information ........................................................................................................... 2

Endpoint Security Introduction .............................................................................................. 10
  Overview of the System Architecture ................................................................................. 10
  Optional System Components ......................................................................................... 11
  Software Blades .................................................................................................................. 12
  Endpoint Security Services and Ports .............................................................................. 12
  Centralized Organization of Users and Computers ......................................................... 13
    Organization-Centric model ........................................................................................... 13
    Policy-centric Model ...................................................................................................... 13
  Centralized Deployment ................................................................................................... 14
  Centralized Monitoring ..................................................................................................... 14
  Related Documentation .................................................................................................... 14

Installing Endpoint Security Servers ...................................................................................... 15
  Planning Endpoint Security Management Server Installation .......................................... 15
  Installation Prerequisites ................................................................................................. 16
  Installing the Endpoint Security Management Server .................................................... 16
    Management Server Configuration - Configuration Tool ............................................... 18
    Management Server Configuration - Endpoint Security Management Console ............. 18
  Users Created during Installation .................................................................................... 19
  Configuring the Apache Cache .......................................................................................... 19
  Viewing Scheduled Tasks .................................................................................................. 19
  Changing the Clean-up Task Status ................................................................................ 19
  Scheduling a New Clean-up ............................................................................................... 20
  Installing Endpoint Security Management Console ......................................................... 20
  Installing External Endpoint Policy Servers ..................................................................... 20
    Policy Server Configuration in the Configuration Tool .................................................. 20
    Policy Server Configuration in the Console .................................................................... 21
  Installing a Server for High Availability ......................................................................... 22
    Secondary Server Configuration in the Configuration Tool ......................................... 22
    Secondary Server Configuration in the Console ............................................................ 22
  Installing a Log Server ...................................................................................................... 24
  Configuring Log Forwarding .............................................................................................. 24
  Upgrading Endpoint Security Servers ............................................................................. 24
  Upgrading Multiple Servers ............................................................................................. 25
  Troubleshooting SIC Trust ............................................................................................... 25

Endpoint Security Licenses .................................................................................................... 27
  Endpoint Security License Types ...................................................................................... 27
  Demo and Product Licenses .............................................................................................. 27
  License Behavior ............................................................................................................... 28
  Getting Licenses ............................................................................................................... 28
  Getting and Applying Contracts ...................................................................................... 28
  License Status .................................................................................................................. 29

Deploying Endpoint Security Clients ..................................................................................... 30
  Deployment Overview ....................................................................................................... 30
  The Initial Client ................................................................................................................. 30
    Getting the Initial Client from the Console ................................................................. 31
    Distributing the Initial Client ....................................................................................... 31
    Seeing the Deployment Status ...................................................................................... 32
  The Software Blade Package ............................................................................................. 32
    Creating a Basic Package .............................................................................................. 32
    Client Packages on the Installation CD ......................................................................... 33
    Global Package Configurations and Content ................................................................. 33
Distributing Software Blade Packages and Updates .................................................. 35
Distributing with Assignments .................................................................................. 35
Distributing by Exporting the Package ...................................................................... 36
Installing the Client Using the CLI .......................................................................... 37
Troubleshooting the Installation ................................................................................ 37
Client logging ............................................................................................................. 38
Uninstalling the Client ............................................................................................... 39
Evaluation Mode Client .............................................................................................. 39

Upgrading Endpoint Security Servers ........................................................................ 41
Upgrading Endpoint Security Servers ........................................................................ 41
Upgrading Multiple Servers ....................................................................................... 42

Upgrading Endpoint Security Clients .......................................................................... 43
Upgrading Clients to E80.30 ....................................................................................... 43
Upgrading with Assignments ...................................................................................... 43
Upgrading with an Exported Package .......................................................................... 44
Gradual Upgrade ......................................................................................................... 44
Upgrading Legacy Clients ........................................................................................... 44
Offline Upgrades ......................................................................................................... 44
Online Upgrades .......................................................................................................... 45

Users and Computers ................................................................................................ 46
Active Directory Scanner ............................................................................................ 46
Configuring the Directory Scanner for the First Time ............................................... 46
Configuring a Directory Scanner Instance .................................................................. 47
Enabling or Disabling a Scanner Instance ................................................................... 48
Directory Synchronization ......................................................................................... 49
Troubleshooting the Directory Scanner ...................................................................... 49
SSL Troubleshooting ................................................................................................... 50
Virtual Groups Overview ............................................................................................ 50
Types of Virtual Groups ............................................................................................. 51
Basic Virtual Groups Management ............................................................................. 51
Adding Objects with an Installation Package .............................................................. 52
Adding Objects from the Monitoring Tab .................................................................. 52
Monitoring Virtual Groups Objects ............................................................................ 53
Role-Based Administration .......................................................................................... 53
Endpoint Security Administrator Roles ....................................................................... 54
Managing Users .......................................................................................................... 57
User Authentication Settings ....................................................................................... 57
Managing OUs or Groups ........................................................................................... 57
Disabling the Preboot Temporarily ........................................................................... 57
Managing Computers .................................................................................................. 58
Managing Users of a Computer .................................................................................. 58
Resetting a Computer ................................................................................................. 59

Using Endpoint Security Management Console ...................................................... 60
Overview Tab ............................................................................................................... 60
My Organization Tab ................................................................................................... 61
Managing Networks ...................................................................................................... 62
Policies Tab ................................................................................................................... 63
Monitoring Tab ............................................................................................................. 63
The Monitoring Toolbar .............................................................................................. 63
Compliance .................................................................................................................. 64
Activity Reports ............................................................................................................ 64
Software Deployment ................................................................................................... 64
Anti-Malware ................................................................................................................ 65
WebCheck ..................................................................................................................... 65
Full Disk Encryption ..................................................................................................... 65
Media Encryption & Port Protection ............................................................................. 66
Versions in Use ............................................................................................................. 67
Custom .......................................................................................................................... 67
Licenses Status Report ................................................................................................. 67
Managing Policies .......................................................... 69
About Policies ................................................................. 69
State of Compliance ......................................................... 70
Non-Compliance ............................................................. 70
Enforcing Policies According to States ......................... 70
User Policy or Computer Policy ..................................... 71
The Heartbeat Interval .................................................... 72
Assigning Policies ............................................................ 72
Direct Assignment ........................................................ 72
Inherited Assignment ..................................................... 73
Policy Assignment Order ................................................. 73
Group Assignment Priority ............................................. 73
Recommendations for Management ............................. 74
Viewing Assignments ...................................................... 75
Deploying Policies ............................................................ 76
Management High Availability ........................................ 77
Overview of High Availability in Endpoint Security .......... 77
The High Availability Environment ................................ 77
Planning for Management High Availability ................. 78
Active versus Standby .................................................... 78
Changing a Server to Active or Standby ....................... 78
Synchronizing the Active and Standby Endpoint Security Management Servers ........................................... 79
What Data is Synchronized? ............................................ 79
Synchronization Status ................................................... 80
When Synchronization Fails ............................................ 80
Understanding the Status of the High Availability Environment ................................................................. 81
Updating the PAT Version on the Server ...................... 81
External Endpoint Policy Servers ...................................... 83
Overview of Endpoint Policy Servers ............................. 83
How do Endpoint Policy Servers Work? ....................... 83
Configuring Policy Server Settings ................................. 84
Endpoint Policy Server Proximity Analysis ..................... 84
Enabling the Management Server to be an Endpoint Policy Server .................................................. 84
Policy Server and Management Server Communication ...... 85
Monitoring Endpoint Policy Server Activity .................... 85
Endpoint Security Active Directory Authentication ............. 87
Configuring Authentication ............................................. 88
Configuring Active Directory for Authentication ............. 88
Configuring Authentication Settings .............................. 89
Troubleshooting Authentication in Server Logs ............... 90
Troubleshooting Authentication in Client Logs ................. 91
Backup and Restore ............................................................ 92
Overview of Backup and Restore .................................. 92
Prerequisites .................................................................. 92
How to Back Up and Restore ........................................ 92
Updating the PAT Version on the Server after Restore .... 93
OneCheck User Settings Policies .......................................... 94
Quick Start ................................................................ 94
Seeing OneCheck User Settings Policy Assignments ....... 95
OneCheck User Settings Assignments ........................... 95
Configuring OneCheck User Settings ............................ 95
Account Lockout ............................................................ 95
Password Security .......................................................... 96
Seeing Full Disk Encryption Policy Assignments .......... 97
Creating a Customized Full Disk Encryption Policy ......... 97
OneCheck User Settings Permissions ............................. 104
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption Policy</td>
<td>106</td>
</tr>
<tr>
<td>Overview of Full Disk Encryption</td>
<td>106</td>
</tr>
<tr>
<td>Quick Start</td>
<td>106</td>
</tr>
<tr>
<td>Preboot Authentication Methods</td>
<td>107</td>
</tr>
<tr>
<td>Global Preboot Authentication Settings</td>
<td>107</td>
</tr>
<tr>
<td>User Preboot Authentication Settings</td>
<td>108</td>
</tr>
<tr>
<td>Before You Configure Smart Card Authentication</td>
<td>109</td>
</tr>
<tr>
<td>Smartcard Scenarios</td>
<td>109</td>
</tr>
<tr>
<td>Notes on Using Smartcards</td>
<td>110</td>
</tr>
<tr>
<td>Changing a User's Password</td>
<td>111</td>
</tr>
<tr>
<td>Creating a Customized Full Disk Encryption Policy</td>
<td>111</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>111</td>
</tr>
<tr>
<td>Preboot Protection</td>
<td>112</td>
</tr>
<tr>
<td>User Acquisition</td>
<td>116</td>
</tr>
<tr>
<td>OneCheck Logon</td>
<td>116</td>
</tr>
<tr>
<td>Policy Assignment</td>
<td>117</td>
</tr>
<tr>
<td>Full Disk Encryption Installation and Deployment</td>
<td>118</td>
</tr>
<tr>
<td>Client Requirements for Full Disk Encryption Deployment</td>
<td>118</td>
</tr>
<tr>
<td>Completing Full Disk Encryption Deployment on a Client</td>
<td>118</td>
</tr>
<tr>
<td>Stages of the Deployment Phase</td>
<td>119</td>
</tr>
<tr>
<td>Primary Full Disk Encryption Components</td>
<td>119</td>
</tr>
<tr>
<td>Full Disk Encryption Recovery</td>
<td>119</td>
</tr>
<tr>
<td>Creating Data Recovery Media Material</td>
<td>120</td>
</tr>
<tr>
<td>Using Data Recovery Media</td>
<td>120</td>
</tr>
<tr>
<td>Upgrading Full Disk Encryption</td>
<td>121</td>
</tr>
<tr>
<td>Upgrading Legacy Full Disk Encryption</td>
<td>121</td>
</tr>
<tr>
<td>Full Disk Encryption Troubleshooting</td>
<td>122</td>
</tr>
<tr>
<td>Using CPinfo</td>
<td>122</td>
</tr>
<tr>
<td>Using CPinfoPreboot</td>
<td>123</td>
</tr>
<tr>
<td>Preboot Issues</td>
<td>124</td>
</tr>
<tr>
<td>Full Disk Encryption Logs</td>
<td>124</td>
</tr>
<tr>
<td>Upgrade Issues</td>
<td>124</td>
</tr>
<tr>
<td>Full Disk Encryption Deployment Phase</td>
<td>124</td>
</tr>
<tr>
<td>Dynamic Mount Utility</td>
<td>125</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection Policy</td>
<td>126</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection Terminology</td>
<td>126</td>
</tr>
<tr>
<td>Access to Media Encryption &amp; Port Protection Policies</td>
<td>126</td>
</tr>
<tr>
<td>Global Settings on the Overview Page</td>
<td>127</td>
</tr>
<tr>
<td>General Properties</td>
<td>127</td>
</tr>
<tr>
<td>Creating Rules for Non-Encrypted Devices</td>
<td>128</td>
</tr>
<tr>
<td>Deleting Files on Read-only Devices</td>
<td>130</td>
</tr>
<tr>
<td>Encrypting Removable Media</td>
<td>130</td>
</tr>
<tr>
<td>Creating Custom Media Authorization Settings</td>
<td>131</td>
</tr>
<tr>
<td>Advanced Media Log</td>
<td>132</td>
</tr>
<tr>
<td>Setting Device Categories to Log</td>
<td>132</td>
</tr>
<tr>
<td>Creating Exceptions to Device Logging</td>
<td>132</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection User Alerts</td>
<td>133</td>
</tr>
<tr>
<td>Media Encryption Sites</td>
<td>133</td>
</tr>
<tr>
<td>Configuring Media Encryption Sites</td>
<td>134</td>
</tr>
<tr>
<td>Converting Legacy Encrypted Devices to Media Encryption</td>
<td>135</td>
</tr>
<tr>
<td>Changing the Group Ranking Order</td>
<td>135</td>
</tr>
<tr>
<td>Firewall Rules Policies</td>
<td>136</td>
</tr>
<tr>
<td>Firewall Rules Policy Options</td>
<td>136</td>
</tr>
<tr>
<td>Protection for Servers</td>
<td>136</td>
</tr>
<tr>
<td>Firewall Rules - Control Icons and Buttons</td>
<td>137</td>
</tr>
<tr>
<td>Firewall Rule Number</td>
<td>138</td>
</tr>
<tr>
<td>Examples of Rule Numbers</td>
<td>138</td>
</tr>
<tr>
<td>Creating Firewall Rules</td>
<td>139</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>140</td>
</tr>
</tbody>
</table>
Group Check Properties ................................................................. 176
Client Profile Check Properties .................................................... 176
Service Pack Check Properties ..................................................... 177
WebCheck ..................................................................................... 178
   Enabling WebCheck ................................................................. 178
   Creating Trusted Sites ............................................................. 178
   Temporarily Disabling WebCheck .............................................. 179
Common Client Settings ................................................................. 180
   Common Client Settings Properties ......................................... 180
   Setting a Common Client Policy .............................................. 180
Remote Help .................................................................................. 182
   Remote Help Types ................................................................. 182
   Process for Remote Help .......................................................... 182
   Providing Full Disk Encryption Remote Help ................................ 183
   Providing Media Encryption & Port Protection Remote Help ........... 183
   Disabling Remote Help ............................................................ 184
Index .............................................................................................. 185
Chapter 1

Endpoint Security Introduction

In This Chapter

Overview of the System Architecture 10
Software Blades 12
Endpoint Security Services and Ports 12
Centralized Organization of Users and Computers 13
Centralized Deployment 14
Centralized Monitoring 14
Related Documentation 14


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 resolve endpoint compliance issues before accessing corporate network

Overview of the System Architecture

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

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

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

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

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

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

---

**Endpoint Security Clients**

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

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

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

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

---

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

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></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>ESP Encrypted</td>
<td>TCP/443</td>
<td></td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection Key Exchange</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption User Acquisition &amp; User credentials</td>
<td>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 or all together. Because different groups, networks, OUs, computers, and users have different security needs, you can configure different blade accordingly.

Centralized Deployment

Software Deployment in the Endpoint Security Management server lets you 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 more information about requirements for this release, see the *Endpoint Security Release Notes* (http://supportcontent.checkpoint.com/solutions?id=sk65921).

Chapter 2

Installing Endpoint Security Servers

In This Chapter
- Planning Endpoint Security Management Server Installation
- Installation Prerequisites
- Installing the Endpoint Security Management Server
- Users Created during Installation
- Configuring the Apache Cache
- Installing Endpoint Security Management Console
- Installing External Endpoint Policy Servers
- Installing a Server for High Availability
- Installing a Log Server
- Configuring Log Forwarding
- Upgrading Endpoint Security Servers
- Upgrading Multiple Servers
- Troubleshooting SIC Trust

See the E80.30 Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk65921) for supported platforms for installation.

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.

- 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 E80.30 Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk65921)).
- 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.

Installation Prerequisites

- Before installing Endpoint Security Management Server, make sure the required ports are free ("Endpoint Security Services and Ports" on page 12).

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 E80.30 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 - 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. You can add licenses at a later time.
5. 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.

6. Click Next.
7. 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.
8. Click Next.
   The internal Certificate Authority initializes with the name in the text box.
9. 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.
10. Click Finish.
11. Click Finish.
12. Click Yes to restart the server.

Management Server Configuration - Endpoint Security Management 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 during Installation

During the server installation, a local user account called CPEP$USER is created automatically. 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_Scheduer\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 activate and deactivate 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 `add` flag.

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

```bash
# cpd_sched_config add NewApacheCacheClean -c ""C:\Program Files\CheckPoint\CPuepm\E80.30\apache22\bin\htcacheclean.exe"" -v "-nt -p""C:\Program Files\CheckPoint\CPuepm\E80.30\apache22\cache"" -1100M"" -e 3600 -r
```

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

*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:

**To install directly from the CD:**

1. Run the setup program directly from the installation CD:
   ```bash
   My_CD_Drive:\Windows\CPclnt\setup.exe.
   ```
2. The Welcome message shows.
3. Click *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 *Yes* to create shortcuts on the desktop.
   - A confirmation message shows.
8. Click *OK* and *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.

**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 *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 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 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 Secondary or Policy Server ("Troubleshooting SIC Trust" on page 25) 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).

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 - 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.
   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 Secondary or Policy Server ("Troubleshooting SIC Trust" on page 25) and then click Initialize.
   e) Click Close.
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:

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

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

You can install a server to function only as a Log Server. The Log Server installation is similar to Endpoint Security Management Server installation.

To install a Log Server:
1. Do the procedure to Install an Endpoint Security Management Server ("Installing the Endpoint Security Management Server" on page 16) with these exceptions:
   a) In the left pane of The Only Unified Security Platform page, select to install these products:
      - Security Management
   b) On the Please specify the Security Management type page, select Log Server.
      - A Check Point R70 Log Server installs.
2. When the installation completes, the Check Point Configuration Tool opens. See Management Server Configuration in the Configuration Tool ("Management Server Configuration - Configuration Tool" on page 18) to understand what to do in each window.

Configuring Log Forwarding

You can forward logs from an Endpoint Security Server to a Log Server.

A Log Server can be one of these:
- Endpoint Policy Server - by default defined as a Log Server
- Endpoint Security Management Server - by default defined as a Log Server
- External R7x Log Server

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

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

Do this procedure for each Endpoint Security Server.

To configure Log Forwarding from an Endpoint Security Server to a Log Server:
1. Open SmartDashboard and connect to the Endpoint Security Management Server.
2. Double-click the Endpoint Security 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 applicable log server (Endpoint Security Management server, Endpoint Policy Server, or R7x Log Server).
5. Click OK.
6. Select Policy > Install Database and install the database on all hosts.

Upgrading Endpoint Security Servers

See the Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk65921) for the supported upgrade paths.

Install this release on all Endpoint Security Management servers and Endpoint Policy Servers. They all must be upgraded before you deploy new clients or upgrade existing clients.

Note - New in this release: During the upgrade, new Endpoint Security client packages are automatically put in the server repository.

When you upgrade the Endpoint Security Management server, all saved Full Disk Encryption policies are re-installed on the clients that they were assigned to. If you saved changes to Full Disk Encryption policies but
do not want the changes to be installed on clients, delete the policies or revert the changes before you upgrade the server.

**To upgrade an Endpoint Security Server to this version:**
1. Download the E80.30 Endpoint Security Server Upgrade package.
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 E80.30 SmartConsole from the Check Point Support Center ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)) or from the Endpoin
   t Security Management Server E80.30 for Windows CD > Windows /CPclnt folder.
7. Double-click setup.exe.
8. When prompted, click Remove to uninstall the R80 or E80.x SmartConsole that you have installed.
9. When it completes, double-click setup.exe again to install the E80.30 SmartConsole.

After a server is upgraded to this version, the server modifies existing Media Encryption & Port Protection policies. This adds new versions of Check Point GO to work with Media Encryption & Port Protection.

**To see which policies were modified:**
1. In the Endpoint Security Management Console, click Install Policies.
2. Go to Policies > Media Encryption & Port Protection.
   The Modified column of changed policies shows Server upgrade.

**Upgrading Multiple Servers**
In an environment with multiple Endpoint Security servers that includes High Availability Endpoint Security Management servers or Endpoint Policy Servers, do the upgrade in this sequence:
1. Upgrade all Endpoint Security Management servers.
   a) Upgrade the Active Endpoint Security Management server.
   b) Before you restart the Active Endpoint Security Management server, run cpstop on all Standby Endpoint Security Management servers.
   c) Restart the Active Endpoint Security Management server.
   d) Upgrade all Standby Endpoint Security Management servers and restart them.
2. Upgrade each Endpoint Policy Server immediately after you upgrade the Endpoint Security Management servers.
   **Note** - An Endpoint Policy Server with a version lower than the Endpoint Security Management Server continues to communicate with clients, but will not synchronize with the newer Endpoint Security Management Server.

**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 an Endpoint 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.
Chapter 3

Endpoint Security Licenses

In This Chapter
- Endpoint Security License Types 27
- Demo and Product Licenses 27
- License Behavior 28
- Getting Licenses 28
- Getting and Applying Contracts 28
- License Status 29

All Endpoint Security licenses are installed on the Endpoint Security Management Server.

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, Compliance Rules, 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>
<tr>
<td>Product</td>
<td>An active license. A Product license must be purchased for each Endpoint Security Software Blade running on the client. Licenses can be purchased as a Subscription, a contract that is renewed annually, or as Per Pay Toll, a one-time purchase.</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 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](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 28).
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](http://usercenter.checkpoint.com)).
2. Click **Products**.
3. Select **Get Contracts File** in the drop-down menu at the right of the row.
4. In the window that opens, save the contract file and click **Open**.
5. Open **SmartUpdate**. ([Start menu > Check Point > SmartUpdate])
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.

## 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.
Chapter 4

Deploying Endpoint Security Clients

In This Chapter

Deployment Overview 30
The Initial Client 30
The Software Blade Package 32
Distributing Software Blade Packages and Updates 35
Troubleshooting the Installation 37
Client logging 38
Uninstalling the Client 39
Evaluation Mode Client 39

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 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 using Software Deployment 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>
<tbody>
<tr>
<td>The Endpoint Security Management Console</td>
<td>• In the Endpoint Security Management Console, go to the Software Deployment tab.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Click Get Initial Client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Distribute to users using third-party distribution software or other method.</td>
<td></td>
</tr>
<tr>
<td>The installation CD</td>
<td>• Get the NEWDA file from CD2 of the Endpoint Security installation package.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Distribute to users using third-party distribution software or other method.</td>
<td></td>
</tr>
<tr>
<td>The Check Point Support Center</td>
<td>Tell users to download the Initial Client from the Support Center (<a href="http://supportcontent.checkpoint.com/solutions?id=sk65921">http://supportcontent.checkpoint.com/solutions?id=sk65921</a>).</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Getting the Initial Client from the 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. Click **OK**.
4. In the **Legacy Uninstall Password** window, click **Skip** (unless you are upgrading a pre-R80 installation).
5. Optional: In the **Add Virtual Group Destination** window, browse to the virtual group for this package.
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 package downloads to the specified location.

**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.
- 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>
</table>
| Software Deployment Assignments | • In the Software Deployment tab, create a new Profile or select an existing profile.  
• Click Assignments.  
• Add all nodes on which you will install the package.  
• Install Policies. | 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. |
| Export Package                  | • In the Software Deployment tab, create a new Profile or select an existing profile.  
• Click Export Package.  
• Choose 32 or 64 bit.  
• Save the package to a directory and distribute it to users as you choose. | 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. |

**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.

**Client Packages on the CD**

<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 administrators.</td>
</tr>
<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>Provide to Client Users from VPN Administrators</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 en 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 nodes that have the policy assigned.
2. Click Add Assignment. The Select Node window opens.
3. In the Select Node window, select an Active Directory or Virtual Groups node. Each node represents an object in the organizational tree.
4. Click OK.
5. Select File > Install Policies or click the Install Policies icon.

#### To remove all Software Blades from a client with Software Deployment:

1. In the Software Deployment tab, click New to create a new Profile.
2. In the tree in the Profile window, click Advanced > Package Settings.
3. In the Package Settings window, click Select.
4. Select the Check Point Endpoint Total Security package and click OK.
5. In the General Properties pane, make sure that no blades are selected.
6. Click OK.
7. Deploy this profile on a client to remove all Software Blades.
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 Groups ("Adding Objects with an Installation Package" on page 52).
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 Window'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></td>
</tr>
<tr>
<td>Reg_SZ</td>
<td>Logging</td>
</tr>
<tr>
<td>Value</td>
<td>voicewarmupx</td>
</tr>
</tbody>
</table>

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

### 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:

  ```
  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
  Reg_SZ                  | Logging
  Value                   | voicewarmupx
  ```
To install or uninstall using the command line, the user must have administrator privileges ("run as administrator").

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

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

Microsoft suggests this solution:

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

See also DES encryption on Windows 7 clients ("Configuring Active Directory for Authentication" on page 88)

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
- Compliance Rules
- Full Disk Encryption
- Media Encryption & 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 Settings\All Users\Application Data\CheckPoint\Endpoint Security\Logs

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

- 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=sk65921) 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.
### Blade or Feature | Comments
--- | ---
**Network Security Features** | - Firewall Rules  
- Compliance Rules  
- 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 256-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.
Chapter 5

Upgrading Endpoint Security Servers

In this Chapter

- Upgrading Endpoint Security Servers
- Upgrading Multiple Servers

You can upgrade Endpoint Security Management Servers and Endpoint Policy Servers to the current version. For a list of supported upgrade paths, see the Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk65921).

**Note** - From version E80.30, during the upgrade, new Endpoint Security client packages are automatically put in the server repository.

Upgrading Endpoint Security Servers

See the Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk65921) for the supported upgrade paths.

Install this release on all Endpoint Security Management servers and Endpoint Policy Servers. They all must be upgraded before you deploy new clients or upgrade existing clients.

**Note** - New in this release: During the upgrade, new Endpoint Security client packages are automatically put in the server repository.

When you upgrade the Endpoint Security Management server, all saved Full Disk Encryption policies are re-installed on the clients that they were assigned to. If you saved changes to Full Disk Encryption policies but do not want the changes to be installed on clients, delete the policies or revert the changes before you upgrade the server.

To upgrade an Endpoint Security Server to this version:

1. Download the E80.30 Endpoint Security Server Upgrade package.
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 E80.30 SmartConsole from the Check Point Support Center (http://supportcenter.checkpoint.com) or from the Endpoint Security Management Server E80.30 for Windows CD > Windows /CPclnt folder.
7. Double-click setup.exe.
8. When prompted, click Remove to uninstall the R80 or E80.x SmartConsole that you have installed.
9. When it completes, double-click setup.exe again to install the E80.30 SmartConsole.

After a server is upgraded to this version, the server modifies existing Media Encryption & Port Protection policies. This adds new versions of Check Point GO to work with Media Encryption & Port Protection.

To see which policies were modified:

1. In the Endpoint Security Management Console, click Install Policies.
2. Go to Policies > Media Encryption & Port Protection.
   - The Modified column of changed policies shows Server upgrade.
Upgrading Multiple Servers

In an environment with multiple Endpoint Security servers that includes High Availability Endpoint Security Management servers or Endpoint Policy Servers, do the upgrade in this sequence:

1. Upgrade all Endpoint Security Management servers.
   a) Upgrade the Active Endpoint Security Management server.
   b) Before you restart the Active Endpoint Security Management server, run `cpstop` on all Standby Endpoint Security Management servers.
   c) Restart the Active Endpoint Security Management server.
   d) Upgrade all Standby Endpoint Security Management servers and restart them.

2. Upgrade each Endpoint Policy Server immediately after you upgrade the Endpoint Security Management servers.

   **Note** - An Endpoint Policy Server with a version lower than the Endpoint Security Management Server continues to communicate with clients, but will not synchronize with the newer Endpoint Security Management Server.
Chapter 6

Upgrading Endpoint Security Clients

In This Chapter

- Upgrading Clients to E80.30
- Upgrading Legacy Clients

This section includes procedure for upgrading endpoint clients to E80.30.

Upgrading Clients to E80.30

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 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 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 **Deployment** tab, select a package and click **Upgrade Profile**. A message opens that shows if an update is available.
2. Click **Yes** to confirm that you want to upgrade the profile.
3. In the **Export Package** window:
   a) Select the platform versions (32/64 bit) to export for laptops and desktops.
   b) Enter or browse to a destination folder.
4. Click **OK**. The package **EPS.msi** and/or **PreUpgrade.exe** files are downloaded to the specified path. A different folder is automatically created for each option selected in step 3a.
5. Send the **EPS.msi** and **PreUpgrade.exe** files to endpoint users. Endpoint users manually install the packages. They must use Administrator privileges.
   You can also use third party deployment software, a shared network path, email, or some other method.

**Gradual Upgrade**

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

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

When you are prepared to upgrade all clients, upgrade all packages.

**Upgrading Legacy Clients**

See the **Endpoint Security Release Notes** (http://supportcontent.checkpoint.com/solutions?id=sk65921) for the supported upgrade paths for this version. Legacy clients are those earlier than version R80. 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**.

**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 E80.30 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**. Select the new profile in the table, and click **Export Package**.
   - The **Uninstall Password** window opens.
5. In the **Legacy Upgrade** area, select **Support legacy upgrade** and enter the passwords needed to uninstall legacy products.
6. 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.
7. Click **OK**.
8. Browse to the location that the package will export to.
9. Click **OK**.
   - The package exports to the chosen location. The `Preupgrade.exe` file is automatically created in the same directory.
10. 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 7

Users and Computers

In This Chapter

- Active Directory Scanner 46
- Virtual Groups Overview 50
- Role-Based Administration 53
- Managing Users 57
- Managing OUs or Groups 57
- Managing Computers 58

Active Directory Scanner

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

When you first log in to 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.

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 related to each Directory Scanner instance requires read permissions to:

- The Active Directory path to be scanned.
- The deleted objects container.

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

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

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

Configuring 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 the scan frequency. One scanner instance can include the full 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.
   The Directory Scanner introduction message opens if you have not yet configured the Directory scanner.
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 47).

Configuring a Directory Scanner Instance

A scanner instance defines which path of the Active Directory will be scanned and the scan frequency. One scanner instance can include the full Active Directory.

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. Go to Endpoint Security Management Console > My Organization tab.
2. From the Tools menu, select Directory Scanner.
   The Directory Scanner Configuration window opens.
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>
</tbody>
</table>
| LDAP Path      | Enter the full LDAP path according to the format: LDAP://<Domain-Controller Host Name>/<Root DN> where:
  - Domain-Controller Host Name: the name of the domain controller.
  - Root DN: The search base root distinguished name. Usually, the distinguished name of the domain name.

  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.

  The directory scanner scans all objects under the selected OU.

  **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 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.
- 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 Active Directory that do not have Endpoint Security are deleted from My Organization.
- Computers deleted from the Active Directory that do have Endpoint Security move to the Other Users/Computers folder because they might require recovery. You can delete these computers manually from the Management Console.
- Objects updated in the Active Directory are also updated on the server.
- Unchanged records stay unchanged.

Troubleshooting the Directory Scanner

<table>
<thead>
<tr>
<th>Problem</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:

  ErrDescr:cpADScanner.CIADs.GetObj(LDAP://<Domain-Controller Host Name>/<Root-DN>),429, Cannot create ActiveX component.
  ErrDescr:cpADScanner.CIADs.GetObj(LDAP://<Domain-Controller Host Name>/<Root-DN>),429, Cannot create ActiveX component.

  Possible causes:
  - Connectivity problems exist between the Endpoint Security server and the Domain Controller.
  - The Directory Scanner does not have permission to search the base object.
  - Incorrect LDAP path.

- Possible cpADscanner entry:

  ErrDescr:cpADScanner.CIADs.GetObj(LDAP://<Domain-Controller Host Name>/<Root-DN>),429, Cannot create ActiveX component.
  ErrDescr:cpADScanner.CIADs.GetObj(LDAP://<Domain-Controller Host Name>/<Root-DN>),429, Cannot create ActiveX component.

  Possible causes:
  Connectivity problems exist between the Endpoint Security server and the Directory Scanner. For example, if the Endpoint Security Server service has stopped or the server has not fully started.
SSL Troubleshooting

During Active Directory instance configuration, you might see a message that is related to SSL configuration. Find the problem and solution here.

**Issue: Stronger authentication is required**

**Solution:**

Try to connect with SSL with these steps:

a) Get an SSL certificate from your Domain Controller.

b) Import the SSL certificate to the Endpoint Security Management server.

c) Open the file: `%UEPMDIR%\engine\webapps\EPS\WEB-INF\application.properties`.

d) Set the `USE_SSL` parameter to true.

e) Set the `LDAP_PORT` parameter exists in this file, set its value to the port of your Active Directory (for example, 636).

**Issue: Wrong SSL Port**

**Solution:**

Open the file `%UEPMDIR%\engine\webapps\EPS\WEB-INF\application.properties` and:

- Change the configured port: Set the `LDAP_PORT` parameter to the SSL port of your Active Directory (for example, 636).

  or

- Disable SSL: Set the `USE_SSL` parameter to false. If the `LDAP_PORT` parameter exists in this file, set its value to the port of your Active Directory (for example, 389).

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

**Solution:**

a) Check the LDAP path of the domain controller in the Directory Scanner Configuration and make sure that an LDAP server is running on the configured machine.

b) Open the file: `%UEPMDIR%\engine\webapps\EPS\WEB-INF\application.properties`. If the `LDAP_PORT` parameter exists in this file, set its value to the port of your Active Directory (for example, 389).

**Issue: SSL certificate is not installed**

**Solution:**

- Create an SSL certificate on your Active Directory server and import it to the Endpoint Security Management server.

  or

- Disable SSL: Open the file: `%UEPMDIR%\engine\webapps\EPS\WEB-INF\application.properties` and set the `USE_SSL` parameter to false. If the `LDAP_PORT` parameter exists in this file, set its value to the port of your Active Directory (for example, 389).

Virtual Groups Overview

Virtual Groups let you create and manage groups, users, and computers with the Endpoint Security Management Console. You can use it with Active Directory for added flexibility or as an alternative to Active Directory.
Organizations can benefit from using Virtual Groups if they:

- Use Active Directory but do not want to use it for Endpoint Security. For example:
  - Different administrators manage the Active Directory and Endpoint Security.
  - Your Endpoint Security requirements are more complex than the Active Directory groups. For example, you want different groups for laptop and desktop computers.
- Use an LDAP tool that is not Active Directory or do not use an LDAP tool.

Virtual Groups behave very much like Active Directory. You can:

- Create groups and then automatically or manually add objects to the groups.
- Assign policies to groups or users.
- Put objects into multiple groups.
- Choose which policies have priority on an endpoint.

**Important** - All environments can manage computers and servers with virtual groups. To manage users with virtual groups you must do one of these:

- Use Full Disk Encryption and enable User Acquisition.
- Import objects into Endpoint Security with an Active Directory Scanner Instance. Afterwards you can move them around manually.

### Types of Virtual Groups

Create new virtual groups in the **My Organization** tab. In the My Organization tree, below Active Directory folders, there is a folder called **Virtual Groups**. Each group shows below the **Virtual Groups** folder in a flat list.

There are three types of virtual groups:

- **Virtual Group** - Can contain users and computers. If objects are in multiple user and computer groups or in a user and computer group and an Active Directory group, you can choose which policies have priority.
- **Computer Group** - Only contains computers. Computers in this group have computer-based policies and the policy of the computer usually has priority over the policy of users who connect to it. If a user has a direct policy assignment, the user's policy has priority. If the computer does not have a policy assigned to it, the policy of the user is active.
- **Server Group** - A type of computer group that only contains Windows servers. Computers in this group have computer-based policies that always have priority over the user policy.

These virtual groups are automatically created and populated:

- **Desktops in My Organization** (Computer Group)
- **Laptops in My Organization** (Computer Group)
- **Servers in My Organization** (Server Group)

If you add objects to a virtual group with an installation package ("Adding Objects with an Installation Package" on page 52), computer objects are not automatically put into these virtual groups.

### Basic Virtual Groups Management

When you create a new virtual group, you set the group type. The group type cannot change after it is set. When you create or delete a virtual group or add or remove objects from a group, the changes are automatically saved and installed immediately.

- Objects can be in multiple groups.
- You can move objects between virtual groups and from Active Directory groups to virtual groups.
- You can copy an Active Directory group to a new virtual group.
To create a new virtual group:
1. In the My Organization tab > My Organization tree, right-click Virtual Groups or an existing virtual group and select New Virtual Group.
2. In the Enforce Changes window, click OK.
3. In the New Virtual Group window:
   - Enter a name for the group in the Display Name field.
   - Optional: Enter a Description of the group.
4. Click OK.

The Active Directory structure is not changed when you copy Active Directory objects or groups into virtual groups.

To add existing objects or groups to a virtual group, do one of these:
- Drag and drop an object or objects from one OU or group to a different group.
- Right-click an OU and select Add Contents to Virtual Group.
  Objects that are part of the OU at the time when you make the change are added to the virtual group. All objects that are added to the OU at a later time will NOT be added automatically to the virtual group.
- In the Monitoring tab, select objects and select Add to Virtual Group from the Monitoring toolbar.

You can select multiple objects with the standard Control + Shift action.

Adding Objects with an Installation Package

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

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

To configure a virtual group destination for an installation package:
1. In the My Organization tab, create the virtual group that the endpoint will be put in.
2. In the Software Deployment tab, select a Profile and click Export Package.
3. In the Platform selection window, select 32-bit or 64-bit. If the package contains only the Initial Client, you can install the 32-bit version on endpoint computers that run 32 bit or 64-bit Windows versions.
4. In the Legacy Uninstall Password window, click Skip (unless you are upgrading a pre-R80 installation).
5. In the Add Virtual Group Destination window, browse to the virtual group for this package.
6. Click OK.
7. Click OK.
8. In the Browse for Folder window, select the location where the package is saved. We recommend that you click Make New Folder and give the folder a descriptive name, such as "Group A Initial Client".
9. Click OK.
  The package downloads to the specified location.

You can add upgraded endpoints to virtual groups from the Monitoring tab.

Adding Objects from the Monitoring Tab

Add users and computer objects to a group from the Monitoring tab with the Add to Virtual Group option. You can select multiple objects from a report and add them to an existing virtual group. You can use the tools in the Monitoring toolbar to filter the Endpoints list and show specified users and computers.
To add objects to a virtual group from the Monitoring tab:

1. Select the users and/or computers to add.

2. In the Monitoring toolbar, click the Options icon and select Add to Virtual Group.
   The Select Virtual Group window opens.

3. Select the group and click OK.

**Monitoring Virtual Groups Objects**

Virtual Groups objects show in Monitoring reports like other objects. You can create groups for specified purposes and also for monitoring.

For example, if you want to try a new Endpoint Security upgrade, you can create a virtual group that contains the endpoints that you upgrade. You can then easily monitor the deployment and activity of those endpoints.

**Role-Based Administration**

After installing the Endpoint Security Management server, you need to assign administrator roles ("Endpoint Security Administrator Roles" on page 54).

**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 54)
   - Help Desk ("Help Desk Role" on page 55)
   - Read Only ("Read Only Role" on page 56)
   - Remote Help (on page 56)

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></td>
<td>Install Policy</td>
<td>Remote Help</td>
</tr>
<tr>
<td>Read Only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Read Only

<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></td>
<td>Install Policy</td>
<td>Remote Help</td>
</tr>
<tr>
<td>Read Only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Read/Write

<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></td>
<td>Install Policy</td>
<td>Remote Help</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Object database Permission on General tab

<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></td>
<td>Install Policy</td>
<td>Remote Help</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</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>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Help Desk Role

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

**Read Only Role**

<table>
<thead>
<tr>
<th>Object database Permission</th>
<th>Remote Help selected on the Endpoint Security tab</th>
<th>The administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Only</td>
<td>Yes</td>
<td>Read Access to the whole system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Save and Install buttons are disabled.</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></td>
<td>No</td>
<td>Save and Install buttons are disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The administrator can only be assigned Remote Help access permissions by an administrator with full access.</td>
</tr>
</tbody>
</table>

**Remote Help**

<table>
<thead>
<tr>
<th>Object Database Permission</th>
<th>The administrator can/cannot:</th>
</tr>
</thead>
<tbody>
<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>
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.
- **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 Detail 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.

**User Authentication Settings**

Change the Preboot authentication method for individual users in the OneCheck User Settings page. This is the authentication method that users use to log in to their computers if the Full Disk Encryption blade is part of their policy.

The default authentication method is Password. From version E80.30 and higher, you can also use Smartcard authentication.

See Preboot Authentication Methods (on page 107) for more details.

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.
- **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. 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 101) 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.
- **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:

   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.
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

Using Endpoint Security Management Console

In This Chapter

Overview Tab 60
My Organization Tab 61
Policies Tab 63
Monitoring Tab 63
Software Deployment Tab 67
Finding Components in the Console 67
Revert to Defaults 68

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 in Endpoint Security Management Console.

To open Endpoint Security Management Console:

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

Overview Tab

The Overview tab shows a general summery of your Endpoint Security deployment.
<table>
<thead>
<tr>
<th>Area</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policies</strong></td>
<td>Shows the number of policies in use for:</td>
</tr>
<tr>
<td></td>
<td>• Software Deployment</td>
</tr>
<tr>
<td></td>
<td>• OneCheck User Settings</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption</td>
</tr>
<tr>
<td></td>
<td>• Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td></td>
<td>• Access Zones</td>
</tr>
<tr>
<td></td>
<td>• Malware Protection</td>
</tr>
<tr>
<td></td>
<td>• Firewall Rules</td>
</tr>
<tr>
<td></td>
<td>• Application Control</td>
</tr>
<tr>
<td></td>
<td>• Compliance Rules</td>
</tr>
<tr>
<td></td>
<td>• WebCheck</td>
</tr>
<tr>
<td></td>
<td>• Common Client Settings</td>
</tr>
<tr>
<td><strong>Monitoring Summary windows 1 and 2</strong></td>
<td>Shows the current status of your endpoints according to user selectable types of status information.</td>
</tr>
<tr>
<td></td>
<td><strong>Browse</strong> button (not available for all report types) lets you filter the summary according to individual user object nodes or groups of nodes.</td>
</tr>
<tr>
<td></td>
<td><strong>Show Details</strong> Shows a detailed view of the selected portion of the report. Sort the view according to specific columns.</td>
</tr>
<tr>
<td></td>
<td>Use the (+) sign in the title bar to clone the monitoring window any number of times.</td>
</tr>
<tr>
<td><strong>License Reports</strong></td>
<td>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 <strong>Show Details</strong>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Getting Started</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Endpoint infections</strong></td>
<td>Provides a summary of infections during the last twenty-four hours.</td>
</tr>
<tr>
<td><strong>Anti-Malware Updates</strong></td>
<td>Shows the anti-malware version currently deployed, and lets you check for available updates.</td>
</tr>
</tbody>
</table>

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

**My Organization Tab**

This tab shows the groups, users, and computer contained within your organization and the policies assigned to each. You can also see the Software Blades configured on each machine and get Monitoring reports for groups.

The organizational structure is shown in the **My Organization** tree. If you import Active Directory information with an Active Directory scan, the information is displayed hierarchically in the tree. All virtual groups and users are shown under the **Virtual Groups** node.
Under the **My Organization** root are these top-level nodes:

<table>
<thead>
<tr>
<th>Node</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|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                                                                                                                                                                 |
|Virtual Groups            | Contains all virtual groups in a flat list.                                                                                                                                                      |
|Other Users/Computers     | Contains:  
  - All users and computers not found in the Active Directory or Virtual Groups, but which exist on the computer on which the Endpoint Security client is installed.  
  - Objects that have been deleted from the Active Directory or Virtual Groups but whose recovery information is retained for possible future use. |

- Double-click a node to show its contents.
- Click the **Highlight** icons at the top of the tree to highlight computers that:  
  - Have policy overrides  
  - Do not have Endpoint Security installed  
  - Have monitoring indications

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Summary</td>
<td>Similar to <strong>Global Monitoring</strong> on the <strong>Overview</strong> tab. Monitoring Summary shows status information according to report type. The report is for the node selected in the organizational tree.</td>
</tr>
<tr>
<td>Software Blades by Computer</td>
<td>Shows the Software Blades installed on the selected profile. You can edit an existing profile, create new profiles, or override the profile completely.</td>
</tr>
<tr>
<td>Policies Assignment</td>
<td>Shows the configured security policies assigned to the currently selected folder, network, group, computer, or user.</td>
</tr>
<tr>
<td>Comments</td>
<td>Provides space for administration notes</td>
</tr>
</tbody>
</table>

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 72).

**Managing Networks**

The nodes of the My Organization tree are filled automatically by an Active Directory scan, or when installed Endpoint Security client connect to the Endpoint Security Management server. 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 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.

**The Monitoring Toolbar**

In each Monitoring report, you can use the Monitoring toolbar to filter the results shown and do other actions. These options are available:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Enter a text string. It searches all columns and results that contain the string are shown.</td>
</tr>
<tr>
<td>Status:</td>
<td>Select a status to filter by. The options are based on the open report. Endpoints with that status are shown.</td>
</tr>
<tr>
<td>In:</td>
<td>Narrow the results to a node or group in the organization. When you click ..., the <strong>Select Node</strong> window opens.</td>
</tr>
<tr>
<td>🙋 Open the selected user or computer.</td>
<td></td>
</tr>
<tr>
<td>🤔 Click to see other options available. Some options are not available for all reports.</td>
<td></td>
</tr>
<tr>
<td>Export to File</td>
<td>Export the report results to an XLS, HTML, or CSV file.</td>
</tr>
<tr>
<td>Toggle chart percentage</td>
<td>Add and remove the percentages shown on the graph.</td>
</tr>
<tr>
<td>Add to virtual group</td>
<td>Add the selected objects to a Virtual Groups group.</td>
</tr>
</tbody>
</table>
### Compliance

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

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

- **Compliance History** - Shows compliance status incidents occurring during the last 24 hours. Click a point in the chart to see 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 be restricted if steps are not done to make it compliant.
- **Observe** - One or more of the compliance rules that is set as Observe is not met. Users do not know about this status and have no restrictions.
- **Restricted** - The computer is not compliant and has restricted access to network resources.
- **Warn** - The computer is not compliant but the user can continue to access network resources. Do the steps necessary to make the computer compliant.
- **Not Available** - The network protection is disabled or not installed.

### Activity Reports

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

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

There are reports that contain information about the computer encryption and reports that contain information about the Preboot.

### Encryption Reports

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

• **Encryption Troubleshooting** - Shows users and computers that might require troubleshooting for disk encryption. You can see the step of the Full Disk Encryption deployment phase that each endpoint computer is in. This information is helpful when it is necessary to find the problem that prevents a computer from becoming encrypted. The status categories are:
  • Initialization
  • Waiting for Policy
- User Acquisition
- Verifying Setup
- Setup protection
- Deliver Recovery file
- Waiting for restart
- Not installed
- Encryption in Progress

**Preboot Reports**

- **Preboot Access 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.

- **Preboot Access Troubleshooting** - Shows users and computers that require troubleshooting for Preboot authentication. The issues are divided into two categories: user settings or Smartcard drivers on the computer.
  - **Computers with Smartcard driver issues.** The status can be:
    - No Smartcard users configured, no drivers installed
    - No drivers installed, Smartcard users configured
    - Driver mismatch
  - **Users with Preboot access issues.** The status can be:
    - Password not configured
    - Certificate not configured
    - Certificate not valid
    - Certificate does not meet requirements

- **Preboot Authentication Methods** - Shows users' configured Preboot authentication method and how they last authenticated. You can sort the results by the configured authentication method. The columns in the report are:
  - **Method Used** - The Preboot authentication method that the user last used.
  - **Method Configured** - The Preboot authentication method configured for the user. This is the configured global **Preboot Authentication Settings**, or if overridden, the user's settings.
  - **Method Configured at** - When the configured method was configured.
  - **Last Preboot Authentication** - When the user last authenticated to an Endpoint Security client computer.
  - **Grace Period Enabled** - If a new authentication method is configured, do users have a period of time that they can still authenticate with the previous method.
  - **Grace Period Active** - Is the grace period active at this time for this user.

**Media Encryption & Port Protection**

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**.

### Revert to Defaults

When an Endpoint Security Management Console tab is open, in the **View** menu > name of open tab, you can select **Revert to Defaults**. This option causes the panes in that tab in the Endpoint Security Management Console to revert to their initial sizes and positions. It does not change the settings or policies.

To revert the panes in a tab of the Endpoint Security Management Console to their default sizes and positions:

1. In the Endpoint Security Management Console, select **View** > name of an open tab > **Revert to Defaults**.
   
   A message opens: **Please restart the application for the changes to take effect.**
   
   When you click **OK**, the Endpoint Security Management Console does not restart automatically.
2. Manually restart the Endpoint Security Management Console for the change to occur in the Console.
Chapter 9

Managing Policies

In This Chapter

About Policies 69
Assigning Policies 72
Deploying Policies 76

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.

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>Compliance Rules</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>
</tbody>
</table>
Common Client Settings | Defines a common policy for multiple endpoint clients. This lets you deploy and maintain many clients efficiently.

**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 ("The Heartbeat Interval" on page 72).

To configure the time period that users have before an endpoint computer is restricted:

1. In the Endpoint Security console, select Manage > General Properties > Connection Settings.
2. In the Out of Compliance section, enter the number of heartbeats.
3. Click OK.

When you configure this time period, we recommend that you give users sufficient opportunity to:

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

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

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

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.

**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 as the **heartbeat interval**.

Note - The default heartbeat interval is 60 seconds.
A heartbeat interval that is too short can cause performance degradation. A heartbeat interval that is too long can cause security degradation and less accurate reporting.

The 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 machine 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**

All container objects in the organizational tree can 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. **Virtual Server Groups** - If a computer is in a Server Group, the policy assigned to it has priority over all policies assigned to users or other groups.
3. **Direct Assignment** - If a User or a Computer is assigned a specific policy, it overrides inherited policies and takes precedence over the following calculations.
4. **Group Ranking** - Each Active Directory or virtual group has a rank. If an entity is in multiple groups, it gets the policy of the highest ranking group.
5. **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.
6. **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 you assign policies to Active Directory or Virtual Groups, conflicts can occur when:

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

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

- **Use global group assignment priority** - Use all policy assignment from the selected group. You can select which group’s policies to use.
- **Blade Priority Assignment/Override global group assignment priority** - Use the policy that you assigned for the blade and not the policies of the group.

   **Note** -
   - Overrides take precedence over Global priority assignment.
   - Virtual Groups show in the priority list in the same way as Active Directory groups.

If you do not configure the priorities before you arrange the groups, a **Group Assignment Priority** window opens when you move objects into groups that have different priorities.

**To set the global group assignment priority:**

1. Open the **Policies** tab.
2. On the **File** menu, select View > Policy Overview > Group Assignments Priority. The **Group Assignments Priority** area opens.
3. From the drop-down box, select **Global**.
   The table shows the current global priority.

4. Click **Change Priority**.
   
   **Note** - This option only shows if a policy is already assigned to the group

   The **Global: Group Assignment Priority** window opens.

5. Use the arrow buttons to move a group up or down.

6. 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 **Policies** tab.
2. On the **File** menu, select **View > Policy Overview > Group Assignments Priority**.
3. The **Group Assignments Priority** area shows.
4. In the **View By** drop-down, select a blade.
5. 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

6. Select **Override global group assignment priority**.
7. Use the arrow buttons to reorder the groups.
8. 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 servers in server groups take precedence over all other policies.
Managing Policies

### Container Object | Assignment Description
---|---
**My Organization** | 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:

- No overriding policy is assigned.
- The Endpoint Security Management Server cannot resolve a lower container or node.
- A user logs into a computer for the first time after client installation, and the client cannot connect to the server.

**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 or virtual 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 polices 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.

If you make changes to an object that relate to Virtual Groups, the changes are enforced immediately. For example, if you move an object into a Virtual Groups group and give the policies of the group priority, they will take effect on the object immediately. However, if you change a policy that is assigned to a Virtual Groups group, the changes to the policy only take effect after you install policies.
Chapter 10

Management High Availability

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 ("Installing a Server for High Availability" on page 22).

The High Availability Environment

The Management High Availability environment requires an Active Endpoint Security Management server and at least one Standby Endpoint Security Management server.

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 Endpoint Security Management server.

**Planning for Management High Availability**

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

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

- **Different physical locations** - It is good to have at least one Standby Endpoint Security Management server in a different location than the Active Endpoint Security Management server 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 81).

- 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 81).

> **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 22).

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, 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. 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** - Endpoint client deployment packages (MSI files) and SmartCard drivers are NOT synchronized. You must manually copy these items 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 Endpoint Security Management server or a Standby Endpoint Security Management server. The Synchronization Status is in the SmartDashboard > **Management High Availability Servers** window in the **status** column or in SmartView Monitor.

The possible synchronization statuses are:

• **Never been synchronized** - 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 Endpoint Security Management server 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 Endpoint Security Management server 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 Endpoint Security Management server 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.

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

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

If the system detects that a large amount of data must be synchronized, it does a full backup, similar to the first synchronization. This can happen after a long period when the servers were disconnected.

### 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 80) 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 change from Standby ESM to Active ESM is planned, (for example, for maintenance), 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 change from Standby to Active was not planned, 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:
   ```bash
   %uepmdir%\bin>uepm patver set <new_PAT_version_number>
   ```
4. Make sure the new PAT version is set by running:
   ```bash
   %uepmdir%\bin>uepm patver get
   ```
Chapter 11

External Endpoint Policy Servers

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.

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

For installation and initial configuration instructions, see Installing External Endpoint Policy Servers (on page 20).

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 Endpoint Policy Servers on the list. The server that replies the fastest is considered to be closest.

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

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

**How the proximity analysis works:**

2. The Endpoint Security Management server pushes the list to the clients.
3. The Device Agent on the client does a proximity analysis after a specified interval to find the Endpoint Policy Server 'closest' to it. Some events in the system can also cause a new proximity analysis. Proximity is based on the response time of a specified HTTP request sent to all servers on the list.
   
   **Note** - Proximity is not based on the physical location of the server. A client in New York will connect to the California Endpoint Policy Server if the California Endpoint Policy Server replies before the New York Endpoint Policy Server.
4. The client tries to connect to the closest Endpoint Policy Server.
5. If a server is unavailable, the Device Agent tries the next closest server on the list until it makes a connection.
6. Based on data contained in the shared list, the client and Endpoint Policy Server create connection URLs.

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

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

Configuring 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 an Endpoint Policy Server**

Configure if the Endpoint Security Management server behaves as an Endpoint Policy Server along with the other Endpoint Policy Servers.
The default is that the Endpoint Security Management server does behave as an Endpoint Policy Server.

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

To configure the Endpoint Security Management server to behave as an Endpoint Policy Server only if all Endpoint Policy Servers do not respond:
1. In 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.**
- **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 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.

**Monitoring Endpoint Policy Server Activity**

You can see the status of Endpoint Policy Servers in the Monitoring tab of 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 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 12

Endpoint Security Active Directory Authentication

In This Chapter

Configuring Authentication 88
Configuring Active Directory for Authentication 88
Configuring Authentication Settings 89
Troubleshooting Authentication in Server Logs 90
Troubleshooting Authentication in Client Logs 91

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.

This option is only available for endpoints that are part of Active Directory.

The authentication process:

1. The Endpoint Security client (2) requests an authentication ticket (1) from the Active Directory server (3).
2. The Active Directory server sends the ticket to the client.
3. The client sends the ticket to the Endpoint Security Management Server.
The default behavior after Security Management Server installation is **Unauthenticated** mode. It is recommended that you use this mode while you are evaluating Endpoint Security, in a lab environment; and that you change to **Strong Authentication** just before moving to a production environment. It is not recommended to continue to work in Unauthenticated mode after moving to production in a live environment.

**Important** - If you use Active Directory Authentication, Full Disk Encryption and Media Encryption & Port Protection are only supported on endpoint computers that are part of Active Directory.

If you have endpoint computers in your environment that are not part of Active Directory, Full Disk Encryption and Media Encryption & Port Protection will not work on them.

### Configuring Authentication

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

**To efficiently move to Strong Authentication:**

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

### Configuring Active Directory for Authentication

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

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

**Important** - In the procedure below you create a user that is mapped to the ktpass service. After you create this user, do not make changes to it, for example, do not change the password. If you do change the user, the key version increases and you must update the **Key version number** in the **Active Directory SSO Configuration** window in the 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**:
     ```plaintext```
     ktpass princ ServiceName/realm@REALM mapuser <userName>@REALM pass <userPass> out <name of outFile>
   ```plaintext```
   - **Example**: 

---
Endpoint Security Active Directory
Authentication

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
keys 74 tst/nac1.com@NAC1.COM ptype 0 (KRB5_NT_UNKNOWN) vno 7 etype 0x17 (RC4-HMAC) keylength 16 (0x32ed87bdc5e9cb88547376818d4)

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>
</tbody>
</table>
| Principle Name         | Provide the name of the authentication service in the format of: SERVICE/realm@REALM
This value must match what was done in Active Directory > New Object. |
| Password               | Provide (and confirm) the password of the Active Directory Domain Admin user you created for Endpoint Security use.                             |
| Ticket encryption method | Select the encryption method according to the Active Directory output.                                                                          |
| Key version number     | Provide the version number according to the Active Directory output.                                                                           |
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 49).

**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:

```
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 88).

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 88).

## Troubleshooting Authentication in Client Logs

The Authentication.log file for each Endpoint Security client is on the client computer at `%DADIR%/logs`.

A normal log is:

```
[KERBEROS_CLIENT(KerberosLogger_Events)] : Credentials acquired for John@ACME-CON
[KERBEROS_MESSAGE(KerberosLogger_Events)] : Message is Empty.
[KERBEROS_CLIENT(KerberosLogger_Events)] : Security context is not yet established.continue needed.
```

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

**No authority could be contacted for authentication.**

The Endpoint Agent cannot find a Domain Controller to supply credentials. To fix this:

1. Make sure that the client is in the domain and has connectivity to your Domain Controller.
2. To authenticate with user credentials, log off and then log in again.
   - To authenticate with device credentials, restart the computer.

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

**The specified target is unknown or unreachable.**

Check the service name. Make sure that there are no typing errors and that the format is correct. If there was an error, correct it in the Check Point Endpoint Security Management.
Chapter 13

Backup and Restore

Overview of Backup and Restore

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

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

The compressed package contains:

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

The migration utility:

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

Prerequisites

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

How to Back Up and Restore

To Back up Endpoint Security data:

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

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

The <output_file_name> can be the output file path. If you do not include an output file path, the utility generates the .tgz file in the %FWDIR%\bin\upgrade_tools directory.
To restore Endpoint Security data:
1. Copy the tgz file from the source server to the target server.
2. Open a command prompt.
3. Change directory to: `%FWDIR%\bin\upgrade_tools`
4. Run `migrate.exe import` with the full path to the input (tgz) file.
   For example: `%FWDIR%\bin\upgrade_tools> migrate.exe import <input_file_name>`
   The migrate utility:
   - Extracts the configuration files from the tgz.
   - Copies them to the correct places.
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 <old_PAT_version_number> + 10`
4. Make sure the new PAT version is set by running:
   `uepmdir%\bin>uepm patver get`
Chapter 14
OneCheck User Settings Policies

In This Chapter
Quick Start 94
Seeing OneCheck User Settings Policy Assignments 95
OneCheck User Settings Assignments 95
Configuring OneCheck User Settings 95

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.

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.

<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>
</tbody>
</table>
### Number of failed attempts before a temporary lockout
The maximum number of failed logon attempts allowed before the user account is temporarily locked out from the computer for a defined duration.

### Duration of a temporary lockout
If the temporary lockout option is selected, this sets the duration of a temporary lockout, in number of minutes.

### Maximum number of successful logons allowed before the account is locked
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.

## 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 Window’s 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. 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.

**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 98)
   - Preboot Protection
   - User Acquisition (on page 102)
   - 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.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 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.

**Low User Trust** | - 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

**Medium User Trust** | - Preboot is enabled  
- Temporary Preboot Bypass is disabled after 2 logon attempts or 2 days  
- Remote Help enabled

**Higher User Trust** | - Preboot is enabled  
- Temporary Preboot Bypass is disabled after 1 automatic logon or 1 day  
- Remote Help enabled

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><strong>Enable USB device in preboot environment</strong></td>
<td>Select to use a device that connects to a USB port. If you use a USB Smartcard you must have this enabled. If you do not use USB Smartcards, you might need this enabled to use a mouse and keyboard during Preboot.</td>
</tr>
<tr>
<td><strong>Enable PCMCIA</strong></td>
<td>Enables the PCMCIA Smartcard reader. If you use Smartcards that require this, make sure it is enabled.</td>
</tr>
<tr>
<td><strong>Enable mouse in preboot environment</strong></td>
<td>Lets you use a mouse in the Preboot environment.</td>
</tr>
<tr>
<td><strong>Allow Serial Over LAN in preboot environment</strong></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><strong>Allow low graphics mode in preboot environment</strong></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 100)
   - Temporary Preboot Bypass (on page 101)
   - Remote Help (on page 102)

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:
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. Warning: 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>
</tbody>
</table>
Bypass failure Preboot message
Enter a message to display to the user if Preboot Bypass fails. For example, to call the Help Desk if the Preboot window opens.

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.

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

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. 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 57).

To configure Temporary Preboot Bypass settings:
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>
</tbody>
</table>
Allow Windows Logon | Lets the user log in to Windows after the Temporary Preboot Bypass logon.

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 Smartcards 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**.
3. The OneCheck Logon widow opens.
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:**

1. Go to the **OneCheck User Settings Policy > Advanced > Password Security** page.
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.

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>
</tbody>
</table>
| Allow user of recovery media          | Let user authenticate to use recovery media to recover and decrypt data from an encrypted system.  
   **Note:** In E80.20 and higher, if this is not selected, users can still access recovery media that is created with a temporary user and password. |
| Allow user to change his credentials from the endpoint client | Let users change the password on an endpoint client during the Preboot. |
| Allow Single Sign-On use              | 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. |

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>
Chapter 15

Full Disk Encryption Policy

In This Chapter

Overview of Full Disk Encryption 106
Quick Start 106
Preboot Authentication Methods 107
Creating a Customized Full Disk Encryption Policy 111
Full Disk Encryption Installation and Deployment 118
Full Disk Encryption Recovery 119
Upgrading Full Disk Encryption 121
Full Disk Encryption Troubleshooting 122

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. 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**.

### Preboot Authentication Methods

If the Preboot is enabled on a computer as part of Full Disk Encryption, the user must enter authentication credentials to log in during the Preboot authentication. In versions E80.30 and higher, users can authenticate to the Preboot with these two methods:

- **Password** - Username and password. This is the default method.
  
  The password can be the same as the Windows password or created by the user or administrator.

- **Smartcard** - A physical card that you associate with a certificate.
  
  Users must have a physical card, an associated certificate, and Smartcard drivers installed as part of the Full Disk Encryption **Preboot Authentication Settings**.

Endpoint Security clients with a version lower than E80.30 must upgrade to use the Smartcard authentication method.

Configure the global settings for the Preboot authentication method from the **Full Disk Encryption Policy Overview** page.

Configure settings for individual users in **User Details > Security Blades > OneCheck User Settings > Modify**.

### Global Preboot Authentication Settings

Configure the global settings for the Preboot authentication method from the **Full Disk Encryption Policy Overview** page. The settings configured there are the settings for all users. However you can override the global settings for individual users in **User Details > Security Blades > OneCheck User Settings > Modify**.

Choose if the default Preboot authentication method is:

- **Password** - Users can only authenticate with a username and password.
- **Smartcard (requires certificates)** - Users can only authenticate with a Smartcard.
- **Either Smartcard or Password** - Users can authenticate with either username and password or Smartcard.

⚠️ **Important** - Before you configure Smartcard authentication as the default, make sure that you understand the requirements. See **Before You Configure Smart Card Authentication** (on page 109). All requirements must be set up correctly for users to successfully authenticate with Smartcards.

### To configure Password authentication only as the default:

1. In the **Policies** tab, select **Full Disk Encryption** from the tree.
2. On the **Full Disk Encryption Policy Overview** page, below **Preboot Authentication Settings**, click **Configure**.
3. In the **Preboot Authentication Settings** page, select **Password** as the **Default Preboot authentication method**.
4. The password settings are taken from the OneCheck User Settings Policy that is assigned to the user. Make sure those settings meet the needs of your organization.
5. Click **OK**.
6. Click **Save and Install**.
7. In the Install Policies window, select Common Settings.
8. Click Install Policies.

To configure Smartcard only or for Smartcard or Password as the default:
1. In the Policies tab, select Full Disk Encryption from the tree.
2. On the Full Disk Encryption Policy Overview page, below Preboot Authentication Settings, click Configure.
3. In the Preboot Authentication Settings page, select one of the Smartcard options as the Default Preboot authentication method.
4. If you select Smartcard, we recommend that you select Change authentication method only after user successfully authenticates with a Smart Card
This lets users authenticate with a password until all of the requirements for Smartcard authentication are set up correctly. After users successfully authenticate one time with a Smartcard, they must use their Smartcard to authenticate. If you configure a user for Smartcard only and do not select this, that user is not able to authenticate to Full Disk Encryption with a password.
Select one or more Smartcard drivers.

5. In the Smartcard driver area, select the Smartcard protocol that your organization uses:
   - Not Common Access Card (CAC) - all other formats
   - Common Access Card (CAC) - the CAC format
6. In the Select Smartcard driver to be deployed area, select the drivers for your Smartcard and Reader. All selected drivers will be installed on endpoint computers when they receive policy updates.
   If you do not see a driver required for your Smartcard, you can:
   - Enter a text string in the Search field.
   - Click Import to import a driver from your computer. If necessary, you can download drivers to import from the Check Point Support Center (http://supportcenter.checkpoint.com).
7. In the Directory Scanner area, select Scan user certificates from Active Directory if you want the Directory Scanner to scan user certificates.
8. If you selected to scan user certificates, select which certificates the Directory Scanner will scan:
   - Scan all user certificates
   - Scan only user certificates containing the Smartcard Logon OID - The OIDs are: 1.3.6.1.4.1.311.20.2.2.
9. Click OK.
10. Click Save and Install.
11. In the Install Policies window, select Common Settings.
12. Click Install Policies.
If necessary, use the Preboot Monitoring reports to troubleshoot issues with drivers or user certificates.

**User Preboot Authentication Settings**

Users get the Preboot authentication method from the global Preboot Authentication Settings. You can override the settings for individual users on the User Details > Security Blades > OneCheck User Settings page. You can also assign a user password and manually add user certificates on this page.

To change a user's Preboot authentication method:
1. Right-click on a user and select Edit.
2. Click OneCheck User Settings from the General Details page or select Security Blades > OneCheck User Settings.
3. See the user’s configured authentication method, for example, "Eva Guerra’s Preboot authentication is Password", and click Modify.
4. In the window that opens, select an option:
   - Use global settings to determine the authentication method for this user - Reverts to the global settings.
   - Use specific authentication settings for this user - Configure a different method for this user.
5. If you selected Use specific authentication settings for this user, select the authentication method:
• Password - This user can only authenticate with a username and password.
• Smartcard (requires certificate) - This user can only authenticate with a Smartcard.
• Either Smartcard or Password - This user can authenticate with either username and password or Smartcard.

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

7. Click OK.

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

9. Click OK.

Before You Configure Smart Card Authentication

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

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

• Smartcard authentication is only supported on Endpoint Security clients of version E80.30 or higher. Make sure all users have a supported version. You can see which versions users have in the Endpoint Security Management Console > Monitoring tab > Versions in Use.

• Users must have the physical Smartcard in their possession.

• Users’ computers must have a Smartcard reader driver and token driver installed for their specific Smartcard. Install these drivers as part of the global Preboot Authentication Settings.

• Each user must have a certificate that is active for the Smartcard. The Directory Scanner can scan user certificates from the Active Directory. Configure this in the global Preboot Authentication Settings.

• You can manually import a certificate for a user in User Details > Security Blades > OneCheck User Settings.

Smartcard Scenarios

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

Scenario 1: Moving from Password to Smartcard

Scenario

Your organization uses Check Point Endpoint Security with username and password authentication for Full Disk Encryption Preboot. You want to move all users to Smartcard authentication for even greater security. Your organization uses Active Directory.

What To Do

1. Plan your Smartcard environment:
   • Give all users a Smartcard.
   • Get a Smartcard certificate for each user and put them in Active Directory.
   • Learn which Smartcard driver and Reader driver is necessary for your Smartcard.
2. Upgrade all endpoints to this version. Use Monitoring reports to make sure all users are successfully upgraded.
4. In the Preboot Authentication Settings window:
   - Select Smartcard (requires certificates).
   - Select Change authentication method only after user successfully authenticates with a Smart Card.
   - Select the drivers required for your Smartcard.
   - Select Scan user certificates from Active Directory.
5. Monitor the Smartcard deployment in the Preboot Monitoring reports.
6. If you choose, you can clear the Change authentication method only after user successfully authenticates with a Smart Card option after all users have logged on with their Smartcard. If a specified user must use password authentication temporarily, you can change the Preboot Authentication Settings for the user to Password.

**Scenario 2: Mix of Password and Smartcard Authentication**

**Scenario**

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

**What To Do**

1. Plan your Smartcard environment.
   - Give a physical Smartcard to all users who will use a Smartcard.
   - Get a Smartcard certificate for each user who will use a Smartcard.
   - Learn which Smartcard driver and Reader driver is necessary for your Smartcard.
2. Deploy the Endpoint Security client, including Full Disk Encryption on all endpoints, as described in the Installing and Deploying Endpoint Security Clients chapter. Use Monitoring reports to make sure that Full Disk Encryption completes the deployment phase and the Full Disk Encryption Status of each computer is Encrypted.
4. Configure the Preboot Authentication Settings in one these ways:
   - a) Configure the global Preboot authentication method as Password and manually Configure the Smartcard users to use Smartcard authentication.
   - b) Configure the global Preboot authentication method as Either Smartcard or Password. For added security, you can manually configure each Smartcard users to use Smartcard authentication only.
5. In the global Preboot Authentication Settings page, select the drivers required for your Smartcard and the Smartcard protocol. All users will receive these settings, including those who are configured to use Password authentication.
6. In the OneCheck User Settings page for each Smartcard user, in the User Certificates area, click Add to import a certificate.
7. Monitor the Smartcard deployment in the Preboot Monitoring reports.

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

**Notes on Using Smartcards**

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

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

To change a user’s Preboot password from 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.

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 98)
   - Preboot Protection
   - User Acquisition (on page 102)
   - 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.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 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 |
### Security Level | Meaning
---|---
**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.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning:</th>
</tr>
</thead>
</table>
| **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.  

| **Low User Trust** | - 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  

| **Medium User Trust** | - Preboot is enabled  
- Temporary Preboot Bypass is disabled after 2 logon attempts or 2 days  
- Remote Help enabled  |
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 Smartcard you must have this enabled. If you do not use USB Smartcards, you might need this enabled to use a mouse and keyboard during Preboot.</td>
</tr>
<tr>
<td>Enable PCMCIA</td>
<td>Enables the PCMCIA Smartcard reader. If you use Smartcards 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.    |

3. Click **Configure** for more granular control over:
   - Preboot Bypass (on page 100)
   - Temporary Preboot Bypass (on page 101)
   - Remote Help (on page 102)
**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:**
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><strong>Maximum failed logons in Windows before Preboot Bypass is disabled</strong></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>
<tr>
<td>Enable location awareness according to network locations</td>
<td>To make sure that the client is connected to the correct network, the computer pings a defined number of IP addresses during the boot process. If none of the IP addresses replies in a timely manner, the computer might have been removed from the trusted network and Preboot Bypass is disabled. The computer reboots automatically and the user must authenticate in Preboot. If one IP address replies, Preboot Bypass remains enabled. <strong>Note:</strong> While this option is enabled, Windows cannot be started in Safe Mode.</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

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. 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 57).

To configure Temporary Preboot Bypass settings:

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 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 Smartcards 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 widow 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:**

1. Go to the **OneCheck User Settings Policy > Advanced > Password Security** page.
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.
- 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</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>service</td>
<td></td>
<td></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
Full Disk Encryption Policy

- 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. Smartcard 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 Smartcards must use the procedure 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 Endpoint Security Management Console, select 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 Recovery Media file or device to the user who will do the recovery.
8. Make sure the user knows:
   - Which username and password to use.
   - How to boot the computer: with a CD or USB device.

Using Data Recovery Media

Use the newly created Full Disk Encryption recovery media to decrypt the failed computer.

To recover an encrypted computer:
1. On the failed computer, run the recovery media from a CD/DVD or bootable USB device.
2. When the Recovery Console Login windows shows, enter the name and password of a user on the recovery media.
   The disk decrypts using partition keys contained in the Recovery Media.
Note - During the decryption process, the client cannot run other programs.

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 (*Upgrading Endpoint Security Clients* on page 43).

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

Upgrading Legacy Full Disk Encryption

See the *Endpoint Security Release Notes* ([http://supportcontent.checkpoint.com/solutions?id=sk65921](http://supportcontent.checkpoint.com/solutions?id=sk65921)) for this version for supported upgrade paths. Before you upgrade, make sure that encryption or decryption are not running.

The upgrade is done through the standard Endpoint Security MSI packages, which can be run manually or through Endpoint Security software deployment.

During the upgrade:

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

To upgrade a client package from Full Disk Encryption EW:

- If you know the Validation Password, do the procedure in Upgrading Clients (*Upgrading Endpoint Security Clients* on page 43).
- If you do not know the Validation Password, do the procedure below.

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

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

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 and higher</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.

Trouble with Smartcards

If there are Smartcard compatibility issues, change the Legacy USB Support setting in the BIOS. If it is enabled, change it to disabled, and if disabled, enable it.

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 HELPMSG command: C:\>net helpmsg <errorcode>

Full Disk Encryption Deployment Phase

Here are some issues that can occur in the Deployment Phase and possible causes and solutions.

Problem: The deployment is stuck at the User Acquisition step.

Causes and Solutions:

1. The User Acquisition policy might say that multiple users must log on to a computer. You can:
   - Change the User Acquisition policy.
   - Instruct users to log on to the computer so Full Disk Encryption can acquire them.
   If User Acquisition is not enabled, at least one user with a password must be assigned to the device.

2. The 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**

In This Chapter

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

Media Encryption & Port Protection policy prevents data leakage 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.

Media Encryption & Port Protection Terminology

- **Endpoint Computer** - A computer with an Endpoint Security client installed and with the Media Encryption & Port Protection Blade active.
- **Storage Device** or **Removable Device** - Removable media devices on which users can save data files. Examples include: USB storage devices, SD cards, CD/DVD media and external disk drives.
- **Peripheral Devices** - Devices on which users cannot save data and that cannot be encrypted. Examples include: keyboards, Bluetooth devices and SmartCard readers.
- **Device Category** or **Device Class** - Industry standard device type that identifies the base functionality of a storage or peripheral device. Device categories let you configure security rules for different types of devices.
- **Media Owner** - By default, this is the user who encrypts the device. If allowed by the policy, a different user can be assigned to be the media owner. This term applies only to users in Active Directory environments.
- **Explorer Utility** - A software program that lets users read encrypted data on protected computers on which the Media Encryption blade is not active or not connected to an Endpoint Security Management server.

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.

Note - Users not connected to the Endpoint Security Management server (offline) can still access encrypted media by supplying the correct password (unless the option has been disabled in the policy).

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>
</tbody>
</table>
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.

Wild Cards for Exceptions
You can use wild cards in the Device Serial Number field but not in the Device ID String begins with field. If you have a set of devices and the serial numbers start with the same characters, use wild cards to create a group that includes the full set.

For example: If you have three devices with the serial numbers 1234ABC, 1234BCD, and 1234EFG, add the serial device number 1234*, with the wild card *. All three devices will use the same settings.

You can use the wild card ?. This character represents one character in the serial number. You can use more than one ? wild card, but only a match in the start of the serial number and a match in the length of the serial number will count.

Examples:

<table>
<thead>
<tr>
<th>Serial Number with Wild Card</th>
<th>Matches</th>
<th>Does Not Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234*</td>
<td>1234AB, 1234BCD, 12345</td>
<td>1233</td>
</tr>
<tr>
<td>1234???</td>
<td>1234ABC, 1234XYZ, 1234567</td>
<td>1234AB, 1234x, 12345678</td>
</tr>
</tbody>
</table>
Settings are enforced in this sequence when they contain serial numbers:

1. Serial numbers containing *
2. Serial numbers containing ?
3. Serial numbers with no wild card.

This means that profiles containing the serial numbers shown here are enforced in this order:

1. 12345*
2. 123456*
3. 123???
4. 123456?
5. 1234567

### Deleting Files on Read-only Devices

You can enable the option to delete files on devices that are configured as read-only. When you enable this option, only deletion is permitted on the non-encrypted device and no other "write" functionality. For example, if you want to let users upload pictures from a removable media device and then delete those files, enable this option. The user cannot copy files from the Endpoint Security client computer to the device.

*Note* - If a device is configured with the read and write options and you select the enable deletion option, the "write" functionality does not become limited to deletion.

To configure deletion only, make sure the write option is cleared for the device in the Custom Device Access Settings window (Advanced > Not Encrypted Media Access > Configure) and do the procedure below.

To enable deletion of files on read-only devices:

1. In the Media Encryption & Port Protection Policy General Properties window, select Control Access to Non-encrypted Devices > Advanced Settings.
2. Select Enable deletion of files on read-only devices.
3. 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>
</tbody>
</table>
| Full              | Users can:  
|                   | - Encrypt removable media for themselves and others  
|                   | - Remove the encryption from the encrypted device  
|                   | - Change the size of the existing encrypted media |
| Medium            | Users can:  
|                   | - Encrypt removable media for only themselves  
<p>|                   | - Change the size of the existing encrypted media |</p>
<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 MediaAuthorization 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:
<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.</td>
</tr>
<tr>
<td></td>
<td>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>

**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.
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".
The client is connected to: | Can you access the device?
The encrypting Endpoint Security Management server | Get access automatically or get access after you enter the password.
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. | Get access after you enter the device's password, when prompted.
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. | You cannot access the device.

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.**
4. Click **OK**.
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.
Chapter 17

Firewall Rules Policies

In This Chapter

Firewall Rules Policy Options 136
Protection for Servers 136
Firewall Rules - Control Icons and Buttons 137
Firewall Rule Number 138
Creating Firewall Rules 139
Advanced Settings 140

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 70), and whether the Connected or Disconnected ("Enforcing Policies According to States" on page 70) policy is in force.

### 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.

### Protection for Servers

Starting with the E80.30 release, these blades can be installed on supported servers in the same way that they are installed on workstations:

- Malware Protection
- Firewall
- Compliance

**Important** - Application Control is not supported on Windows Server.

**To disable Application Control on servers:**

a) Assign the server group or members to a new application control policy.
b) Disable application control in the policy.
c) Install the policy.
If you install Malware Protection and Firewall Rules policies on servers, it is best for the policies to be machine-based and not user-based. In machine-based policy, the policies assigned to the machine have priority over the policies assigned to users who connect to the machine.

To enforce machine-based policies, we strongly recommend that you put all servers in a server virtual group ("Types of Virtual Groups" on page 51).


## 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>
</tbody>
</table>
| Source and Destination | Source and Destination can be any of the Network Objects defined in the Access Zones policy or the Trusted/Internet Zone.  
  - Source location of network traffic. For an outbound rule, the source will always be the LocalComputer.  
  - Destination location of network traffic. For an inbound rule, the destination will always be the LocalComputer.                                                                                             |
| Service              | Network protocol or service used by traffic.                                                                                                                                                                                                                                                                                               |
| Action               | Effect of the rule on matched traffic: Accept or Drop.                                                                                                                                                                                                                                                                                     |
| Track                | Record Endpoint Security client behavior when the rule is enforced:  
  Log - record rule enforcement in the Endpoint Security client log.  
  Alert - display pop-up on the endpoint computer and record rule enforcement in the Endpoint Security client log.  
  Note: For tracking to work, Firewall logs must be enabled in the Common Client Settings policy.  
  None - log and alert messages are not generated.  
  If you have a rule that drops or accepts all traffic, do not enable logging.                                                                                                                                   |
<p>| Icon/Button          | Action                                                                                                                                                                                                                                                                                                                                   |
| Add Rule at the Bottom | 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. |
| Add Rule at the Top   |                                                                                                                                                                                                                                                                                                                                          |
| Add Rule below Current |                                                                                                                                                                                                                                                                                                                                          |
| Add Rule above Current |                                                                                                                                                                                                                                                                                                                                          |
| (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 &gt; Delete Rule.                                                                                                                                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>(To add a new rule)</th>
<th>To create a new rule (Host, Address Range, Site or Network):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Right-click the table heading row of General Properties &gt; New Rule &gt; Inbound or Outbound. A new Inbound or Outbound rule is added at the top of the table of rules.</td>
</tr>
<tr>
<td></td>
<td>• Right-click a rule row &gt; New Rule &gt; Inbound or Outbound &gt; Above or Below. The new Inbound or Outbound rule is added to the current row.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit</th>
<th>After modifying a firewall rule, the policy must be installed on the Endpoint before it takes effect.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(To disable a rule)</th>
<th>After disabling a firewall rule, the rule no longer affects the client. You might prefer to disable rules rather than delete and recreate them later. Remember that the altered policy must be installed before the change takes effect.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deleting a firewall rule automatically removes it from the Security Policy. However, the Policy must be reinstalled before the change affects endpoint computers.</td>
</tr>
</tbody>
</table>

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>
<tr>
<td>2</td>
<td>FTP Local</td>
<td>Private Subnet</td>
<td>LocalMachine</td>
<td>FTP</td>
<td>Accept</td>
<td>Log</td>
<td></td>
</tr>
</tbody>
</table>

*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**.
To specify the type of tracking, right click the **Tracking** cell and select Alert, Log, or None.

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 18

Access Zones Policies

In This Chapter

- Trusted Zone 141
- Network Objects 142
- Creating New Access Zones Definitions 145
- Changing an Existing Access Zones Policy 145

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.

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.

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 Firewall Rules policy.

- LocalMachine_Loopback
  Endpoint computer's loopback address: 127.0.0.1. The Endpoint must always have access to its own loopback address.

  Note - Endpoint users must not run software that changes or hides the local loopback address, for example personal proxies that enable anonymous internet surfing.

Objects in the Trusted Zone

Think about adding these objects to your Trusted Zone:

- Remote host computers accessed by your programs (if not included in the subnet definitions for the corporate network)
- Corporate WANs accessed by your programs
- Endpoint Security Management Server
- Domain name servers
Access Zones Policies

- 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 these types:
   - Host ("Configuring a Host as a Network Object" on page 143)
   - Address Range ("Configuring an Address Range as a Network Object" on page 143)
   - Network ("Configuring a Network as a Network Object" on page 143)
   - Site ("Configuring a Site as a Network Object" on page 144)
   - Group ("Configuring a Group as a Network Object" on page 144)
   - Network Group with Exclusion ("Configuring a Network Group With Exclusion" on page 144)
   - Site Group ("Configuring a Site Group as a Network Object" on page 145)
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 from the **Available Objects** column, or create new objects.

Configuring a Network Group With Exclusion

Enter data that defines the network object:

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

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

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
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 142).
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:

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 19

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 updates Anti-malware definitions from a Check Point update server.

Prerequisites

Before configuring Malware Protection, you must:

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

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

2. Open `%uepmdir%\engine\conf` and edit the `local.properties` file.
   
   **Note** - Delete the `#` character from the beginning of each row that you edit.
3. Add these properties:
   
   a) The proxy server's IP address as shown in the example below:
      
      `http.proxy.host=<IP address>`
   
   b) The proxy server's listening port as shown in the example below:
      
      `http.proxy.port=8080`
   
   c) The username if basic authentication is enabled on the proxy server. Leave it empty if no authentication is required.
      
      `http.proxy.user=<username>`
   
   d) The password if basic authentication is enabled on the proxy server.
      
      `http.proxy.password=<password>`
4. Save the `%uepmdir%\engine\conf\local.properties` file.
Allowing Malware Protection Update Traffic
After configuring the proxy server, configure the firewall gateway to accept the traffic to the update servers.

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

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

Protection for Servers
Starting with the E80.30 release, these blades can be installed on supported servers in the same way that they are installed on workstations:

- Malware Protection
- Firewall
- Compliance

⚠ Important - Application Control is not supported on Windows Server.

To disable Application Control on servers:

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

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

To enforce machine-based policies, we strongly recommend that you put all servers in a server virtual group ("Types of Virtual Groups" on page 51).


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:
1. On the Endpoint Security Management Server console, open the **Policies** tab and click **Malware Protection** from the **Navigation** tree.
   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:**

1. On the Endpoint Security Management Server console, open the **Policies** tab and click **Malware Protection** from the **Navigation** tree.
   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**.

### 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: &lt;br&gt;&lt;ul&gt;&lt;li&gt;<strong>Custom</strong>&lt;br&gt;Applies settings configured in the <strong>Custom Scan Level Settings</strong> window (<em>Custom Scan Level Settings</em> on page 150). &lt;/li&gt;&lt;li&gt;<strong>Low Scan Level</strong>&lt;br&gt;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.&lt;/li&gt;&lt;li&gt;<strong>Medium Scan Level</strong>&lt;br&gt;Scans all critical areas.&lt;br&gt;Scans local, removable, and CD drives.&lt;br&gt;Skips compressed files and non-executable files.&lt;/li&gt;&lt;li&gt;<strong>High Scan Level</strong>&lt;br&gt;Scans all critical areas.&lt;br&gt;Scans local, removable, CD, and all other drives.&lt;br&gt;Scans all files on the computer.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
</tbody>
</table>
## Option | Description
---|---
### Scan Schedule Settings
Select from these scan schedule options:
- **Scan monthly**
  Schedules one scan a month at the specified time.
- **Scan weekly**
  Schedules one scan a week at the specified time.
- **Scan daily**
  Schedules a scan every day at the specified time.
Click **Configure** to set a date for the first scan and the time of day that scans will occur.

### Scan Treatment Settings
Select how Endpoint Security handles infected files:
- **Repair the file. If repair fails, delete** - If Endpoint Security cannot repair the file it deletes it.
- **Repair the file. If repair fails, quarantine** - 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.

### 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** ("Scan Exclusion and Processes" on page 152) 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 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>
</tbody>
</table>
|                                       | • Quick Scan  
  Scans the Windows folder, subfolders, and startup items. |
|                                       | • Normal Scan  
  Scans all files except compressed files and non-executable files. |
|                                       | • Deep Scan  
  Scans all file types. |
| **Scan Targets**                      | Select from these scan targets: |
|                                       | • **Removable** - Scans removable media devices, such as USB. |
|                                       | • **CD-ROM** - Scans CD-ROMs. |
|                                       | • **Other** - Any device which Windows recognizes as a drive. |
| **Do not scan files larger than**     | Do not include files above a certain size if scanning them significantly decreases computer performance. |
| **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 Signatures and Engine Updates**

You can define these settings of the **Engine and Signature Updates**:  
- Frequency, in hours, between client requests for malware signature and scanning engine updates.  
- The server that the client updates from.  
- The connection time out, after which the update source is considered unavailable.

**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 **OK**.

Clients can get malware updates from their Endpoint Policy Server or an external source. Clients that are not connected to the Endpoint Policy Server usually get updates from an external source.

**To select which server updates the clients:**
1. Go to the **Malware Protection Policy** window.  
2. Open an existing policy or create a new policy.  
3. In the **Malware Signatures and Engine Updates Settings** area, click **Advanced Settings**.  
4. In the **Malware Signature and Engine Update Settings** page:  
   - To get updates from the Endpoint Security Management server or configured Endpoint Policy Server, select **Update from the Endpoint Policy Server**.  
   - To get updates from an external source, that is a specified URL:  
     (i) Select **Update from the following external source**.  
     (ii) Enter the external source URL. The default URL is: **http://kav8.zonealarm.com**.
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.

5. Click OK.

**Note** - If you clear the Update from the following external source option, disconnected clients cannot updates.

To set the period after which the update source is considered to be unavailable:

1. Go to the Malware Protection Policy window.
2. Open an existing policy or create a new policy.
3. In the Malware Signatures and Engine Updates Settings area, click Advanced Settings.
4. In the Malware Signature and Engine Update Settings page, select a value for the Updater connection timeout in seconds. The default value is 60 seconds.
5. Click OK.

**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\n   - 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 an 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**.

**Submitting Malware and False Detections**

Reporting suspected malware or false detections to Check Point helps to improve the security and protection of all Internet users.

If you think that you have malware in your organization that was not detected by Malware Protection, contact Check Point Technical Support. If Malware Protection mistakenly identifies a file as malware, contact Check Point Technical Support.
Chapter 20

Application Control Policies

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:

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

### 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 is 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:

**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 your 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?

### 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.

### 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. 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>Impact area</td>
<td>Level</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>-------------</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.
### 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>
<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>

### 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**.

**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 Window 95, 98, or ME operating systems, you also need to copy `unicows.dll`, located in the `<installdir>checkpoint\Integrity\engine\websapps\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.

**Appscan Switches and Functions**

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/o</code></td>
<td>Specifies the output file to be created. If no file name is specified, the default output file name (<code>scan.xml</code>) is used.</td>
</tr>
<tr>
<td><strong>Example 1:</strong> <code>C:\appscan /o scan1.xml [files]</code></td>
<td></td>
</tr>
<tr>
<td>In Example 1, the scan is named <code>scan1</code>. The output file name is used when importing it into the Endpoint Security Management Server.</td>
<td></td>
</tr>
<tr>
<td>If you conduct multiple scans on the same computer, give each scan a unique name.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| <code>/x</code> | 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 <code>/s</code> switch. |
| • If the <code>/x</code> switch is not used in the command statement: Only program files (.exe file name extension) are scanned. |
| <strong>Example 2:</strong> <code>C:\appscan /o scan2.xml /x &quot;*.exe;*.dll&quot; /s &quot;C:&quot;</code> |
| In Example 2, the scan is named <code>scan2</code>, and the scan will include <code>.exe</code> and <code>.dll</code> files in the current directory only. |</p>
<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
</tr>
</thead>
</table>
| /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 21
Compliance

In This Chapter

Compliance Status 168
Protection for Servers 169
Quick Start 169
Planning Compliance Rules 169
Creating a Compliance Rules Policy 170
Viewing Compliance Rules Policy Assignments 170
Compliance Rules Policy 170
Compliance Rules Assignment 172
Check Object 173

The 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.

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 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.
Protection for Servers

Starting with the E80.30 release, these blades can be installed on supported servers in the same way that they are installed on workstations:

- Malware Protection
- Firewall
- Compliance

⚠️ Important - Application Control is not supported on Windows Server.

To disable Application Control on servers:

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

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

To enforce machine-based policies, we strongly recommend that you put all servers in a server virtual group ("Types of Virtual Groups" on page 51).


Quick Start

This section explains how to quickly assign predefined Compliance Rules policies.

These Compliance Rules 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:

2. Double-click one of the predefined policies. The Compliance Rules 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 ("Compliance Rules Assignment" on page 172) 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 policies 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 Compliance Rules Policy

This section explains how to create an Compliance Rules 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 **Compliance Rules Policy** window opens.
6. Configure the compliance settings.
7. Click **OK**.
8. Click **Save & Install**.

### Viewing Compliance Rules 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**.

### Compliance Rules Policy

This section explains how to configure Compliance Rules 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 ("The Heartbeat Interval" on page 72)
     
     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 87)
**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><strong>Endpoint Security Client</strong></td>
<td>Monitors the client's version. Click <strong>Manage</strong> 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><strong>OS Service Packs and Updates</strong></td>
<td>Checks operating system service packs and updates. Click <strong>Manage</strong> 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 the presence of:  
  - 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></td>
</tr>
</tbody>
</table>
  - Alert the user about non-compliance and provide remediation resources  
  - Log to the administrator |
### Action | Meaning
--- | ---
Restrict | • Alert the user about non-compliance and provide remediation resources  
• Log to the administrator  
• Change relevant polices to the restricted type after a pre-defined number of heartbeats. Before that happens, the user is in the *about to be restricted* state. On the monitoring tab, the user is shown as *pre-restricted*.

**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 a Compliance Rules 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.

### Compliance Rules Assignment

For compliance to work, Compliance Rules 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.

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. If the file exists, the endpoint computer is compliant for the required file.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Registry key and value do not exist</strong> - Make sure the registry key and value does not exist. If the key does not exist, the endpoint computer is compliant for an application that is prohibited.</td>
</tr>
<tr>
<td>Registry Key</td>
<td>Enter the registry key to identify.</td>
</tr>
<tr>
<td>Registry Value</td>
<td>Enter the registry value that matches the Check Registry type.</td>
</tr>
</tbody>
</table>
Check File | Select one of these to check if an application is running or if a file exists:

- **File is running at all times** - For example, make sure that Endpoint Security client is always running.
- **File exists** - For example, make sure that the user browsing history is always kept.
- **File is not running** - For example, make sure that DivX is not used.
- **File does not exist** - For example, make sure that a faulty dll file is removed.

| File Name | Enter the name of the file to find. It can be any file, but if we want the file to run or not run, you must enter the name of the process. (either .exe or .bat) |
| File Path | • Enter the path, but do not include the file name.  
• The **Use environment Variables of logged in user** attribute includes paths defined in the endpoint computer's system and user variables. |
| Check File Properties | Additional options to check for an existing or non-existing file. |
| Match File Version | Make sure that a specific version or range of versions of the file or application complies with the file check. |
| Match MD5 Checksum | Find the file by MD5 Checksum. Click **Calculate** to compare the checksum on the endpoint with the checksum on the server. |
| File is not older than | Find the file by the number of days on the endpoint computer. |

### 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>Option</th>
<th>Description</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

<table>
<thead>
<tr>
<th>Automatically execute operation without user notification</th>
<th>Run the executable file without displaying a message on the endpoint computer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute operation only after user notification</td>
<td>Run the executable file only after asking approval.</td>
</tr>
<tr>
<td>Use same message for both Non-Compliant and Restricted messages</td>
<td>Select that the same text be used for both messages.</td>
</tr>
<tr>
<td></td>
<td>A Non-Compliant message tells the user that the endpoint computer is non-compliant and provides details of how to achieve compliancy.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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 opens.
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.
   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 Windows 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>
Chapter 22

WebCheck

In This Chapter

- Enabling WebCheck ........................................ 178
- Creating Trusted Sites ..................................... 178
- Temporarily Disabling WebCheck ....................... 179

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.


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 178) 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.
4. On the General Properties page, select Enable WebCheck. 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 23

Common Client Settings

In This Chapter

Common Client Settings Properties 180
Setting a Common Client Policy 180

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 Groups, 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>
<tr>
<td>Client Notification</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>Section</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client Install / Uninstall</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>Settings</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>Client Uninstall Password</td>
<td></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 Minimum number of events before attempting an upload</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>Maximum number of events to upload</td>
<td>Desktop Firewall</td>
</tr>
<tr>
<td></td>
<td>Maximum age of event before upload</td>
<td>Application Control</td>
</tr>
<tr>
<td></td>
<td>Discard event if older than</td>
<td>Malware Protection, compliance)</td>
</tr>
<tr>
<td></td>
<td></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>

5. In the navigation tree, select **Assignment**.
6. The **Assignment** page shows.
7. 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.
8. 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.
9. Click **OK**.
10. Select **File > Save**.
Chapter 24

Remote Help

In This Chapter

Remote Help Types 182
Process for Remote Help 182
Providing Full Disk Encryption Remote Help 183
Providing Media Encryption & Port Protection Remote Help 183
Disabling Remote Help 184

Remote Help Types

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 Smartcards, 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 • 67
Access to Media Encryption & Port Protection Policies • 124
Access Zones Policies • 139
Account Lockout • 93
Active Directory Scanner • 44
Active versus Standby • 76
Activity Reports • 62
Adding Network Objects • 140
Adding Objects from the Monitoring Tab • 50
Adding Objects with an Installation Package • 50
Advanced Media Log • 130
Advanced Settings • 138
Anti-Malware • 63
Application Control Policies • 151
Appscan Switches • 161
Assigning Policies • 70

B

Backup and Restore • 90
Basic Virtual Groups Management • 49
Before You Configure Smart Card Authentication • 107

C

Centralized Deployment • 13
Centralized Monitoring • 13
Centralized Organization of Users and Computers • 13
Changing a Server to Active or Standby • 76
Changing a User's Password • 109
Changing an Existing Access Zones Policy • 143
Changing Group Definitions • 159
Changing the Clean-up Task Status • 18
Changing the Group Ranking Order • 133
Check Object • 170
Client logging • 36
Client Packages on the Installation CD • 31
Client Profile Check Properties • 173
Client Requirements for Full Disk Encryption Deployment • 116
Common Client Settings • 177
Common Client Settings Properties • 177
Completing Full Disk Encryption Deployment on a Client • 116
Compliance • 62, 165
Compliance Rules Assignment • 169
Compliance Rules Policy • 167
Compliance Status • 165
Configuring a Client Package with a Default VPN Site • 32
Configuring a Directory Scanner Instance • 45
Configuring a Group as a Network Object • 142
Configuring a Host as a Network Object • 141
Configuring a Network as a Network Object • 141
Configuring a Network Group With Exclusion • 142
Configuring a Site as a Network Object • 141
Configuring a Site Group as a Network Object • 142
Configuring Active Directory for Authentication • 86
Configuring an Address Range as a Network Object • 141
Configuring Authentication • 86
Configuring Authentication Settings • 87
Configuring Log Forwarding • 22
Configuring Media Encryption Sites • 132
Configuring OneCheck User Settings • 93
Configuring Policy Enforcement • 69
Configuring Policy Server Settings • 82
Configuring Software Signatures • 32
Configuring the • 70
Configuring the Apache Cache • 18
Configuring the Directory Scanner for the First Time • 44
Configuring the Proximity Analysis Interval • 82
Configuring VPN Client Settings • 34
Converting Legacy Encrypted Devices to Media Encryption • 133
Creating a Basic Package • 30
Creating a Compliance Rules Policy • 167
Creating a Customized Full Disk Encryption Policy • 95, 109
Creating a Malware Protection Policy • 146
Creating an Appscan • 160
Creating Application Control Configuration • 151
Creating Custom Media Authorization Settings • 129
Creating Custom Program Groups • 158
Creating Data Recovery Media • 118
Creating Exceptions to Device Logging • 130
Creating Firewall Rules • 137
Creating New Access Zones Definitions • 143
Creating Rules for Non-Encrypted Devices • 126
Creating Trusted Sites • 175
Custom • 65
Custom Check and Application Compliance Check Properties • 170
Custom Rules • 169
Custom Scan Level Settings • 147

D

Deleting Files on Read-only Devices • 128
Deleting Program Groups • 159
Demo and Product Licenses • 25
Deploying Endpoint Security Clients • 28
Deploying Policies • 74
Deployment Overview • 28
Direct Assignment • 71
Directory Synchronization • 46
Disabling Remote Help • 181
Disabling the Preboot Temporarily • 55
Distributing by Exporting the Package • 34
Distributing Software Blade Packages and Updates • 33
Distributing the Initial Client • 29
Distributing with Assignments • 33
Drive Encryption • 95, 109
Understanding the Status of the High Availability Environment • 79
Uninstalling the Client • 37
Unknown Program Configuration - Use Case • 155
Updating the PAT Version on the Server • 79
Updating the PAT Version on the Server after Restore • 91
Upgrade Issues • 122
Upgrading Clients to E80.30 • 41
Upgrading Endpoint Security Clients • 41
Upgrading Endpoint Security Servers • 23, 39
Upgrading Full Disk Encryption • 119
Upgrading Legacy Clients • 42
Upgrading Legacy Full Disk Encryption • 119
Upgrading Multiple Servers • 24, 40
Upgrading with an Exported Package • 42
Upgrading with Assignments • 41
User Acquisition • 100, 114
User Authentication Settings • 55
User Policy or Computer Policy • 70
User Preboot Authentication Settings • 106
Users and Computers • 44
Users Created during Installation • 17
Using CPinfo • 120
Using CPinfoPreboot • 120
Using Data Recovery Media • 118
Using Endpoint Security Management Console • 58
Using Program Advisor with a Proxy Server • 164

V

Versions in Use • 65
Viewing Assignments • 74
Viewing Compliance Rules Policy Assignments • 167
Viewing Program Advisor Recommendations • 163
Viewing Scheduled Tasks • 18
Virtual Groups Overview • 48

W

WebCheck • 63, 175
What Data is Synchronized? • 77
When Synchronization Fails • 78
Wild Cards for Exceptions • 127