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=11939
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 April 2011</td>
<td>Multiple AD domains (&quot;Directory Scanner&quot; on page 19)</td>
</tr>
<tr>
<td></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 R80.10 Administration Guide).
# Contents

**Important Information**.........................................................................................3  
**Introduction**........................................................................................................8  
  Overview of the System Architecture ................................................................. 9  
  Endpoint Security Services and Ports ............................................................... 10  
  Software Blades .................................................................................................. 11  
  Centralized Organization of Users and Computers ............................................. 11  
    Organization-Centric model ............................................................................ 11  
    Policy-centric Model ....................................................................................... 12  
  Centralized Deployment ..................................................................................... 12  
  Centralized Monitoring ...................................................................................... 12  
**Installing Endpoint Security Management Server** ............................................ 13  
  Planning Endpoint Security Management Server Installation ....................... 13  
  Prerequisites for Installation ............................................................................ 14  
  Installing the Server .......................................................................................... 14  
  Users Created at Installation ............................................................................ 15  
  Configuring the Apache Cache ......................................................................... 15  
    Viewing Scheduled Tasks ............................................................................... 15  
    Changing the Clean Up Task Status ............................................................. 16  
    Scheduling a New Clean up ........................................................................... 16  
  Installing External Endpoint Policy Servers .................................................... 16  
  Installing Endpoint Security Management Console ....................................... 16  
  Endpoint Security Licenses .............................................................................. 17  
    Endpoint Security License Types ................................................................ 17  
    Demo and Product Licenses .......................................................................... 17  
    License Behavior .......................................................................................... 18  
    Getting Licenses ......................................................................................... 18  
    Getting and Applying Contracts ................................................................ 18  
    License Status .............................................................................................. 19  
  Directory Scanner ............................................................................................... 19  
    Setting Directory Scanner Credentials ......................................................... 19  
    Configuring the Directory Scanner ............................................................... 20  
    Directory Synchronization ............................................................................ 21  
    Troubleshooting the Directory Scanner Configuration .................................. 21  
**Backup and Restore** ......................................................................................... 23  
  Prerequisites ..................................................................................................... 23  
  How to Back Up and Restore .......................................................................... 23  
  Updating the PAT Version on the Server after Restore .................................... 24  
**Using Endpoint Security Administrator Console** ........................................... 25  
  Overview tab ..................................................................................................... 26  
  My Organization Tab ......................................................................................... 26  
    Changing a User's Logon Preboot Password ................................................. 27  
    Managing Networks ....................................................................................... 27  
  Policies Tab ....................................................................................................... 28  
  Monitoring Tab ................................................................................................ 28  
    User Defined Report ..................................................................................... 29  
    Compliance Status ....................................................................................... 29  
    Activity Reports .......................................................................................... 29  
    Software Deployment ..................................................................................... 29  
    Anti-Malware ................................................................................................. 30  
    WebCheck .................................................................................................... 30  
    Full Disk Encryption ...................................................................................... 30  
    Media Encryption & Port Protection .............................................................. 30
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
</tr>
<tr>
<td>31</td>
</tr>
<tr>
<td>31</td>
</tr>
<tr>
<td>32</td>
</tr>
<tr>
<td>32</td>
</tr>
<tr>
<td>33</td>
</tr>
<tr>
<td>33</td>
</tr>
<tr>
<td>34</td>
</tr>
<tr>
<td>34</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>36</td>
</tr>
<tr>
<td>36</td>
</tr>
<tr>
<td>37</td>
</tr>
<tr>
<td>37</td>
</tr>
<tr>
<td>38</td>
</tr>
<tr>
<td>38</td>
</tr>
<tr>
<td>39</td>
</tr>
<tr>
<td>41</td>
</tr>
<tr>
<td>44</td>
</tr>
<tr>
<td>44</td>
</tr>
<tr>
<td>45</td>
</tr>
<tr>
<td>45</td>
</tr>
<tr>
<td>45</td>
</tr>
<tr>
<td>46</td>
</tr>
<tr>
<td>46</td>
</tr>
<tr>
<td>47</td>
</tr>
<tr>
<td>47</td>
</tr>
<tr>
<td>48</td>
</tr>
<tr>
<td>48</td>
</tr>
<tr>
<td>48</td>
</tr>
<tr>
<td>50</td>
</tr>
<tr>
<td>50</td>
</tr>
<tr>
<td>50</td>
</tr>
<tr>
<td>51</td>
</tr>
<tr>
<td>51</td>
</tr>
<tr>
<td>51</td>
</tr>
<tr>
<td>52</td>
</tr>
<tr>
<td>53</td>
</tr>
<tr>
<td>53</td>
</tr>
<tr>
<td>54</td>
</tr>
<tr>
<td>54</td>
</tr>
<tr>
<td>55</td>
</tr>
<tr>
<td>55</td>
</tr>
<tr>
<td>55</td>
</tr>
<tr>
<td>55</td>
</tr>
<tr>
<td>56</td>
</tr>
<tr>
<td>56</td>
</tr>
<tr>
<td>56</td>
</tr>
<tr>
<td>56</td>
</tr>
<tr>
<td>57</td>
</tr>
<tr>
<td>58</td>
</tr>
<tr>
<td>59</td>
</tr>
<tr>
<td>59</td>
</tr>
<tr>
<td>59</td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>62</td>
</tr>
<tr>
<td>Section</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Planning Application Control</td>
</tr>
<tr>
<td>Program Permission Lifecycle Use Case</td>
</tr>
<tr>
<td>Unknown Program Configuration - Use Case</td>
</tr>
<tr>
<td>Phase 1: Block Internet Zone Servers Only</td>
</tr>
<tr>
<td>Phase 2: Block All Servers</td>
</tr>
<tr>
<td>Phase 3: Block All Non-trusted Communication</td>
</tr>
<tr>
<td>Phase 4: White Listing</td>
</tr>
<tr>
<td>Monitoring Applications - Automatic Add</td>
</tr>
<tr>
<td>Creating Custom Program Groups</td>
</tr>
<tr>
<td>Changing Group Definitions</td>
</tr>
<tr>
<td>Deleting Program Groups</td>
</tr>
<tr>
<td>Managing Unknown Applications</td>
</tr>
<tr>
<td>Program Permissions and Disconnected Policies</td>
</tr>
<tr>
<td>Importing Programs</td>
</tr>
<tr>
<td>Scanning Computers</td>
</tr>
<tr>
<td>Manually Adding Programs</td>
</tr>
<tr>
<td>Program Advisor</td>
</tr>
<tr>
<td>Program Advisor Server</td>
</tr>
<tr>
<td>Viewing Program Advisor Recommendations</td>
</tr>
<tr>
<td>Using Program Advisor with a Proxy Server</td>
</tr>
<tr>
<td><strong>Endpoint Compliance</strong></td>
</tr>
<tr>
<td>Compliance Status</td>
</tr>
<tr>
<td>Quick Start</td>
</tr>
<tr>
<td>Planning Compliance Rules</td>
</tr>
<tr>
<td>Creating a Endpoint Compliance Policy</td>
</tr>
<tr>
<td>Viewing Endpoint Compliance Policy Assignments</td>
</tr>
<tr>
<td>Endpoint Compliance Policy</td>
</tr>
<tr>
<td>General Configuration</td>
</tr>
<tr>
<td>Custom Rules</td>
</tr>
<tr>
<td>Endpoint Compliance Assignment</td>
</tr>
<tr>
<td>Check Object</td>
</tr>
<tr>
<td>Custom Check and Application Compliance Check Properties</td>
</tr>
<tr>
<td>Remediation Objects and Client Remediation Messages</td>
</tr>
<tr>
<td>Group Check Properties</td>
</tr>
<tr>
<td>Client Profile Check Properties</td>
</tr>
<tr>
<td>Service Pack Check Properties</td>
</tr>
<tr>
<td><strong>WebCheck</strong></td>
</tr>
<tr>
<td>Enabling WebCheck</td>
</tr>
<tr>
<td>Creating Trusted Sites</td>
</tr>
<tr>
<td>Temporarily Disabling WebCheck</td>
</tr>
<tr>
<td><strong>Common Client Settings</strong></td>
</tr>
<tr>
<td>Common Client Window</td>
</tr>
<tr>
<td>Setting a Common Client Policy</td>
</tr>
<tr>
<td><strong>Remote Help</strong></td>
</tr>
<tr>
<td>Remote Help Types</td>
</tr>
<tr>
<td>Process for Remote Help</td>
</tr>
<tr>
<td>Providing Full Disk Encryption Remote Help</td>
</tr>
<tr>
<td>Providing Media Encryption &amp; Port Protection Remote Help</td>
</tr>
<tr>
<td>Disabling Remote Help</td>
</tr>
<tr>
<td><strong>Index</strong></td>
</tr>
</tbody>
</table>
Chapter 1

Introduction


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

Features:

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

In This Chapter

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

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

### Endpoint Security Management Server

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

### Endpoint Security Clients

<table>
<thead>
<tr>
<th>Number</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><strong>Endpoint Security clients</strong> - Client application installed on end-user computers. These clients monitor the security aspects of your endpoints and enforce security policies.</td>
</tr>
</tbody>
</table>
Endpoint Security Services and Ports

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

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

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

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

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

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

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

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

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

The Endpoint Security Management Server includes these modular, centrally managed software blades. You can enable and configure these blades at any time to meet changing security needs.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| OneCheck User Settings        | Handles:  
  - How an Full Disk Encryption user logs in to the computer  
  - How failed log ins are handled  
  - Password security  
  - Access to remote help.                                                                                                                                                                                                                                                                                                                                                                               |
| Full Disk Encryption          | Combines preboot protection, boot authentication, and strong encryption to ensure only authorized users are granted access to information stored in desktops and laptops.                                                                                                                                                                                                                                                                                       |
| Media Encryption & Port Protection | Protects data stored on the computers by encrypting removable media devices and allowing tight control over computers' ports (USB, Bluetooth, and so on).                                                                                                                                                                                                                                                                     |
| Access Zones                  | Defines the topology of the organizational network, separating it into Trusted and Internet domains.                                                                                                                                                                                                                                                                                                                                                   |
| Malware Protection            | Protects clients from known and unknown viruses, worms, Trojan horses, adware, and keystroke loggers.                                                                                                                                                                                                                                                                                                                                            |
| Firewall Rules                | Blocks or allows network traffic based on attributes of network connections.                                                                                                                                                                                                                                                                                                                                                                               |
| Application Control           | Restricts network access on a per-application basis, allowing you to restrict network access between a particular application and the defined Access Zones.                                                                                                                                                                                                                                                                                      |
| Endpoint Compliance           | Ensures that protected computers comply with your organization's requirements and allows you to assign different security levels according to the compliance state of the endpoint computer. For example, non-compliance may result in a remediation message, a warning, or restriction from the network.                                                                                                                                                     |
| WebCheck                      | Protects endpoint computers against phishing attacks. WebCheck creates its own virtual browser with its own file system. Changes made by a non-trusted site are confined to the virtual browser file system.                                                                                                                                                                                                                           |

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. As different groups, networks, OUs, machines, or users develop different security needs, adjust the different blade configurations accordingly.

Centralized Deployment

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

Centralized Monitoring

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

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

Installing Endpoint Security Management Server

For the current release, you can install Endpoint Security Management Server on Windows 2003 or 2008 Enterprise server platforms. Before starting the installation, make sure the Windows server exists as an object in the Active Directory.

In This Chapter

Planning Endpoint Security Management Server Installation 13
Prerequisites for Installation 14
Installing the Server 14
Users Created at Installation 15
Configuring the Apache Cache 15
Installing External Endpoint Policy Servers 16
Installing Endpoint Security Management Console 16
Endpoint Security Licenses 17
Directory Scanner 19

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 machine for each remote site, and that large sites have multiple Endpoint Policy Servers to ensure good performance.

A

1

B

1

2
Prerequisites for Installation

Before installing Endpoint Security Management Server, make sure the following ports are free ("Endpoint Security Services and Ports" on page 10).

Installing the Server

To install Endpoint Security Management Server for the first time:

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. Select New installation.
5. Click Forward.
6. In the Management area, select
   - Security Management
   - Endpoint Security
   - SmartConsole
7. Click Forward.
8. Confirm installation of selected products and click Forward.
   Follow the installation status for Security Management, Endpoint Security, and SmartConsole.
9. When prompted to select clients for SmartConsole, leave all the options selected.
   Follow the setup status for SmartConsole clients.
10. Click Finish.
   The Check Point Configuration Tool opens for the initial configuration of Endpoint Security products.

Note - You can modify this configuration at a later date by clicking Start > Run > Check Point Configuration Tool, or by typing cpconfig on the command line.

The configuration tool opens on the Licenses and Contracts window.
11. Click Fetch from File (if you have a license file), or leave it blank to use the Evaluation license.
12. Click Next.
13. In the Administrators window, add a user name and password for Endpoint Security administrators.

   Note - Do not modify the default permissions.
14. Click OK.
15. Click Next.
   The Certificate Authority window opens.
16. Click Next.
Users Created at Installation

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

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

Configuring the Apache Cache

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

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

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

Using the cpd scheduler configuration tool you can:

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

Viewing Scheduled Tasks

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

```
# cpd_sched_config print
```

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\CPShared\<version_number>\reserved\CPD_Schedular\ApacheCacheClean
```
Changing the Clean Up Task Status

1. To stop the cache clean up, run:
   
   ```bash
   # cpd_sched_config deactivate ApacheCacheClean -r
   ```

2. To start the cache clean up, run:
   
   ```bash
   # 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:
   
   ```bash
   # 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\R80.10\apache22\bin\htcacheclean.exe\"" -v "-nt -p\"C:\Program Files\CheckPoint\CPuepm\R80.10\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 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 a Endpoint Security Management Server according to the server installation procedures.
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
   - SmartConsole

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:
   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.

Endpoint Security Licenses
Licenses are installed only 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, Endpoint Compliance, Application Control, Anti-Malware, and VPN.) 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>
</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 validation occurs when the client sends either a SYNC or heartbeat messages to the server.
- License expiration dates of the Endpoint Security Software Blades are downloaded to the client.
- License deactivation is supported through the Endpoint Security Management Server console.
- When there is no container license, software blade registration is blocked.

Getting Licenses

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

To get the license for your Endpoint Security Management Server:

1. Log in to Check Point User Center ([http://usercenter.checkpoint.com](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 18).
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-quotiation 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)
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.

---

**Directory Scanner**

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

**Setting Directory Scanner Credentials**

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

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

- All Active Directory containers from the root of the scanned Domain.
- The deleted objects container.

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

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

To set the Scanner credentials:
1. Make sure the Endpoint Security Management Server is installed on a computer listed in the Active Directory
2. Add an account with read permission to the Deleted Objects container to the Domain Admin group or Domain User group.
4. Click Set Credentials.
5. Enter the Domain, account, and password details for the user defined in step 2.
6. Click OK.
7. When prompted, restart the console.

Configuring the Directory Scanner

Before running the Directory scanner you need to create a scan instance. A scan instance defines which branch of the AD should be scanned and how often. One scan can also include the entire AD.

To create a scan instance:
1. Open the Endpoint Security Management Console > My Organization tab.
2. From the Tools menu, select Directory Scanner.
   The Directory Scanner Configuration window opens.
3. Click Add.
   The Directory Access Credentials window opens.
4. Enter the directory access credentials:
   • Domain
   • DC Host (Domain Controller host)
   • User name (of an account with the required credentials)
   • Password
5. Click OK.
   The Directory Scanner Configuration window opens.
6. Fill in these fields.

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

Note - If a defined search base contains AD groups with members that are not in this search base, the scanner will scan these members. To prevent scanning outside the defined OU, create an AD account with permissions for this OU and its children.
Field | Description
---|---

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 **Status** for a specific scan instance can be **New**, **Active**, or **Inactive**.
- The **Scan Status** can be **New**, **Pending**, **Scanning**, or **Periodical**.

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

**Directory Synchronization**

At the specified interval, the Directory Scanner synchronizes Endpoint Security nodes in the **My Organization** tree with nodes in the Active Directory. When synchronization occurs:

- New Active Directory objects are added to Endpoint Security and inherit a policy according to the Endpoint Security policy assignment calculation.
- Deleted users are removed from the **My Organization** tree, but only if they had no encrypted removable media devices. Deleted users with encrypted removable media devices move to the **Other Users/Computers** folder. Even though the user no longer exists in the Active Directory, the server keeps the encryption keys for possible recovery.
- Computers deleted from the AD that do not have Endpoint Security are deleted from **My Organization**.
- Computers deleted from the AD that do have Endpoint Security move to the **Other Users/Computers** folder because they may require recovery. You can delete these computers manually from the Management Console.
- Objects updated in the Active Directory are also updated on the server.
- Unchanged records remain unchanged.

**Troubleshooting the Directory Scanner Configuration**

<table>
<thead>
<tr>
<th>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 Directory Scanner account 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:**
  ```plaintext
  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 the 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.
Chapter 3

Backup and Restore

In This Chapter

Prerequisites 23
How to Back Up and Restore 23
Updating the PAT Version on the Server after Restore 24

Prerequisites

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

How to Back Up and Restore

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

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

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

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

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

Using Endpoint Security Administrator Console

The Endpoint Security Management Console is an integrated Check Point Console.

To open the Endpoint Security Management Console:

Start > All Programs > Check Point SmartConsole R70 > Endpoint Security Management

or:

From a different Check Point console: Windows menu > Endpoint Security Management Console.

The console displays central security management topics in tabbed windows.

In This Chapter

Overview tab 26
My Organization Tab 26
Policies Tab 28
Monitoring Tab 28
Software Deployment Tab 31
Finding Components in the Console 31
Overview tab

The overview tab provides a general summary of your Endpoint Security deployment.

<table>
<thead>
<tr>
<th>Area</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</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 Logon</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>- Endpoint Compliance</td>
</tr>
<tr>
<td></td>
<td>- WebCheck</td>
</tr>
<tr>
<td></td>
<td>- Common Client Settings</td>
</tr>
<tr>
<td>Monitoring Summary windows 1 and 2</td>
<td>Shows the current status of your endpoints according to user selectable types of status information.</td>
</tr>
<tr>
<td></td>
<td>My Organization button (not available for all report types) lets you filter the summary according to individual Active Directory nodes or groups of nodes.</td>
</tr>
<tr>
<td></td>
<td>Show Details Shows a detailed view of the selected portion of the report. Sort the view according to specific columns. Use the (+) sign in the title bar to clone the monitoring window any number of times.</td>
</tr>
<tr>
<td>License Reports</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 Show Details.</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>Getting Started</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>Endpoint infections</td>
<td>Provides a summary of infections during the last twenty-four hours.</td>
</tr>
<tr>
<td>Anti-Malware Updates</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 your environment in a hierarchy organization (tree structure) model where your AD server information is displayed. Use the My Organization tab to manage the security of endpoint computers via the active directory objects (Organizational Units (OUs), groups, computers, and users).

Under the My Organization root are three top-level nodes:
Node | Purpose
--- | ---
Directories | After scanning an Active Directory, this node is populated with the Active Directory tree structure. The middle pane of the **My Organization** tab displays the list of groups, users and computers in the folder or group. Format: `<domain name>_All Groups` - Contains all groups found by the directory scan. The groups are displayed both where they occur in the tree structure and in this special container.

Networks | Networks organized by IP range

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

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Purpose</th>
</tr>
</thead>
<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 related to the node selected in the organizational tree. <strong>Note:</strong> These reports are not available for users, machines, and AD groups.</td>
</tr>
<tr>
<td>Software Blades by Machine</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>Lists policy assignment types</td>
</tr>
<tr>
<td>Comments</td>
<td>Provides space for administration notes</td>
</tr>
</tbody>
</table>

The Policy Assignment pane shows the configured security policies assigned to the currently selected folder, network, group, computer, or user.

A specific user or machine 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 50).

### Changing a User’s Logon Preboot Password

**To change a user's password:**

1. Go to the My Organization tab and double click on the user whose password you want to change. The **User Details** window is displayed.
2. In the left pane, click **User Logon Preboot Settings**.
3. In the **User Logon Preboot Settings** window, click **Change Password**, and the **Change User Password** window is displayed.
4. Enter the new password and enter it again in the appropriate text boxes.
5. Click **OK**.

### Managing Networks

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

**To create a My Organization Network:**

1. Open the **My Organization** tab.
2. Right-click **Networks** and select **New Address Range**.
The Address Range Properties window opens.

3. Provide a name to identify this address range as a managed network.
4. Provide the first IP address and the last IP address of the range.
5. Add a descriptive comment, and select a color.
6. Click **Save**.

### Policies Tab

An **Endpoint Security policy** is a collection of security rules that enforce a specific type of protection. A policy is typically associated with a specified software blade, which must be installed and licensed. The Policies tab lets you define and configure policy rules for different blades.

The left-hand tree shows a list of blades. The tables in the right-hand pane shows the policies assigned to these blades. Clicking the **Overview** option in the left-hand tree shows two tables:

- Policy Assignment per blade
- Modification, save, and installation dates for all policies.
- Group Assignment Priority.

Click View > Policy Overview > Group Assignment Priority. Group Assignment Priority (on page **51**) lets you configure which groups have higher priority when assigning policies.

### Monitoring Tab

The Monitoring tab shows a variety of security related data. Sort this data according to different criteria to generate reports on the status of endpoint computers.

**To see reports in the Endpoint Security Management Server:**

1. On the **Endpoint Security Management Console**, select the Monitoring tab.

The navigation tree shows the type of report available for each blade:

<table>
<thead>
<tr>
<th>Report type</th>
<th>Monitoring Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Defined</td>
<td>Create custom reports by selecting criteria</td>
</tr>
<tr>
<td>Compliance status</td>
<td>Select criteria from the <strong>Status</strong> Drop-down box</td>
</tr>
<tr>
<td>Activity Reports</td>
<td>• Protected by Endpoint Security</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Connectivity</td>
</tr>
<tr>
<td></td>
<td>• Top infections</td>
</tr>
<tr>
<td>Software Deployment</td>
<td>• Deployment Status</td>
</tr>
<tr>
<td></td>
<td>• Deployment by Package</td>
</tr>
<tr>
<td></td>
<td>• Deployment by Profile</td>
</tr>
<tr>
<td>Anti-malware</td>
<td>• Anti-malware Provider Brands</td>
</tr>
<tr>
<td></td>
<td>• Anti-malware Scanned Date</td>
</tr>
<tr>
<td></td>
<td>• Anti-malware Status</td>
</tr>
<tr>
<td>WebCheck</td>
<td>• WebCheck Status</td>
</tr>
<tr>
<td></td>
<td>• WebCheck History</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>• Full Disk Encryption Status</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption Troubleshooting</td>
</tr>
<tr>
<td>Media Encryption &amp; Port Protection</td>
<td>Select criteria from the <strong>Status</strong> drop-down box</td>
</tr>
</tbody>
</table>
### User Defined Report

Use this page to create reports that put together different monitoring criteria.

- Click **Choose monitoring criteria** to select sort options
- Use the **Show Endpoint that** drop-down box to show data that match all or any of the selected criteria

### Compliance Status

Use this page to show endpoint compliance status:

- Compliant
- About to be restricted
- Observe
- Restricted
- Warn
- All

**Compliance History** - Shows a line chart of the number of compliance status incidents occurring in the last 24 hours. Click one of the items in the legend on the right to show the number of incidents for that status.

### Activity Reports

The Activity report shows connectivity data for the client during the past two weeks.

The pie chart shows the percentage of:

- Unprotected computers connected during the last 15 minutes
- Last hour
- Last 24 hours
- Last 30 minutes
- Computers that connected more than 24 hours ago
- All

Hovering the mouse above an item in the legend box, such as unprotected computers, causes the pie chart to highlight the related data.

### Software Deployment

Shows the current Endpoint Security deployment status for endpoint clients:

- Completed
- Deploying
- Downloading
- Failed
- Uninstalling

Hover the mouse above an item in the Legend to highlight the related area of the pie chart.
Anti-Malware
Shows the current status of Malware Protection.

WebCheck
- **WebCheck Status** - Shows the current WebCheck monitoring status for individual clients in terms of:
  - Disabled
  - Enabled
  - Not installed
  - User disabled
  - All

Full Disk Encryption
Shows the current Full Disk Encryption status in terms of:
- Encrypted
- Decrypting
- Not installed
- Unencrypted
- Encrypting
- System setup
- All

The troubleshooting pages covers:
- Initialization
- Setup Protection
- User Acquisition
- Setup verification
- Deliver recovery file
- Waiting for a policy
- Waiting for restart
- Not installed
- Encryption in progress
- All

Media Encryption & Port Protection
This page shows the Media Encryption & Port Protection status in terms of:
- Allowed devices
- Authorized devices
- Blocked Devices
- Unauthorized Devices
- All
Versions in Use

This page covers which versions are in use:

- **Full Disk Encryption** - Shows the installed version of the Full Disk Encryption blade for individual 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.

Software Deployment Tab

You use this tab to:

- Configure and deploy software blades
- 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

After you set up your Endpoint Security environment, there are components that most administrators will need to find for maintenance and troubleshooting, such as endpoints, users, directories, and programs.

The Endpoint Security Management Console provides a search feature for these components.

**To find a basic component:**

1. In the tool bar, provide a string to match a component.
2. In the drop-down list, select either My Organization Search (to find a computer, user, or directory of computers or users) or Program Control Search.
3. Click Search.
   The Search Results window opens.
4. If the component you are looking for is listed, select it and click Navigate to Result.

   **Note** - Alternatively, right-click any user shown on the Monitoring tab > Navigate to > User or Machine.
Chapter 5

Installing and Deploying Endpoint Security Clients

Configure and distribute your Endpoint Security clients to your endpoint computers. This must be done before policies can be deployed on endpoints.

Follow this workflow:

1. Install and configure the server.
2. Customize and create policies according to your needs.
   After monitoring the status of endpoints, you can create policies with customized rules for behavior, and then install the policies for quick organization-wide security configurations.
3. Install the policies ("Deploying Policies" on page 53). At this stage, the policies are deployed in the system and are made available for the endpoint clients. Policies are enforced on the endpoints after the endpoints have downloaded them from the server.
4. Configure the client packages that you need. ("Configuring Client Packages" on page 36)
   a) Create the properties of a client profile ("Handling Client Packages" on page 44).
   b) If you use VPN, configure the default VPN site.
   c) Configure Signature Settings ("Providing Software Signatures" on page 38).
   d) If you are ready for Strong Authentication ("Understanding Endpoint Security Authentication" on page 39), configure Authentication Settings.
      It is recommended that you first configure the client for a pilot installation, without authentication. When you are ready to move to production, configure new clients with authentication.
5. Export the profile as a client package ("Exporting Packages" on page 41) and send the package to the endpoint users with GPO, SMS, or other distribution method.

In This Chapter

Installing the Client Using the EPS.msi File 32
Installing the Client Using the CLI 33
Client logging 33
Troubleshooting the Installation 34
Uninstalling the Client 35
Client Packages 35
Configuring Client Packages 36

Installing the Client Using the EPS.msi File

An exported client can be installed or upgraded by double-clicking the EPS.msi file. However:

- Double-clicking the msi will 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.
- A blade cannot be added to an existing client installation manually by double-clicking the msi file. To add a blade, use the command line options.
Endpoint Agent Installations and Upgrades

When installing or upgrading an Endpoint Agent, remember that:

- An msi file that contains only an Endpoint Agent cannot be installed on a computer that already has a client installed.
- To rollback to a client that only contains an Endpoint Agent, assign a policy with no blades. Make sure the DA remains the same version.
- You cannot upgrade only the Endpoint Agent if the Agent has blades. Agent and blades must be upgraded together.

Installing the Client Using the CLI

Command line Option | Meaning
--- | ---
msiexec /i <path to EPS.msi> | Do a fresh installation
msiexec /i <path to EPS.msi> | Add an initial blade or blades
msiexec /i <path to EPS.msi> REINSTALL=DUMMY REINSTALLMODE=voums | Add or remove blades
msiexec /i <path to EPS.msi> | Upgrade using the indicated package.

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>voicewarmupx</td>
</tr>
</tbody>
</table>

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

Client logging

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

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

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

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

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

- Uploaded according to the Common Client Policy ("Setting a Common Client Policy" on page 120) 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 R80 Endpoint Security User Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11778) for more about what clients can do with logs on their computers.

**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:

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

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

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

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

  Microsoft suggests two possible solutions:

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

  Microsoft suggests two possible solutions:
### 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.

### Client Packages

After you have configured the Software Blades, the system automatically installs the blades into the correct client package. There are four types of package:

- Evaluation
- Master full
- Master full without network protection
- New Endpoint Agent

Each package has a 32 and 64 bit version. All packages are named **EPS.msi**.

---

### Microsoft Solution | Explanation

| KB311269 | Register the WScript object by running the `wscript -regserver` command from a command prompt or from the Run option on the Start menu. |
| KB20027 | Make sure Scrrun.dll is installed on the endpoint computer, and that it is correctly registered. To register the dll:
- Open a command prompt
- Change directory to `c:\windows\system32`
- Run: `Regsvr32 scrrun.dll`

- See also DES encryption on Windows 7 clients (*Configuring Active Directory for Authentication* on page 42)

### 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 remedy:

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
### Configuring Client Packages in Detail

<table>
<thead>
<tr>
<th>Directory Name on CD</th>
<th>Package description</th>
<th>Software Blades contained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master_EVAL</td>
<td>Evaluation mode client, 32 and 64 bit versions</td>
<td>Endpoint Connect VPN (default), SecureClient VPN, Firewall Rules, Anti-malware and WebCheck, Application Control, Access Zones, Endpoint Compliance, Full Disk Encryption, OneCheck User Settings, Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td>Master_EVAL_x64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master_FULL</td>
<td>Full package, 32 and 63 bit versions. Full package</td>
<td>Endpoint Connect VPN (default), SecureClient VPN, Firewall Rules, Anti-malware and WebCheck, Application Control, Access Zones, Endpoint Compliance, Full Disk Encryption, OneCheck User Settings, Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td>Master_FULL_x64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master_FULL_NO_NP</td>
<td>Check Point Media Encryption &amp; Port Protection and Full Disk Encryption</td>
<td>Endpoint Connect VPN (default), SecureClient VPN, WebCheck, Access Zones, Full Disk Encryption, OneCheck User Settings, Media Encryption &amp; Port Protection</td>
</tr>
<tr>
<td>Master_FULL_NO_NP_x64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEWDA</td>
<td>Endpoint agent, 32 and 64 bit versions</td>
<td>None.</td>
</tr>
<tr>
<td>NEWDA_x64</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When preparing the client, unnecessary Software Blades already in the assigned package are automatically deleted.

---

### Configuring Client Packages

In the **Software Deployment** tab, you configure a package profile. This defines the properties and global settings that will be included in the installation of a selected MSI package.

**To configure a package 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, color for the profile object, and optional comment to identify this set of deployment settings.
4. In the **General Properties > Software Blades** field select the blades to install.
5. Select the **Assignment** branch.
6. In the **Assignment** field select which **Nodes** in the Network to assign the Profile for deployment.
7. Select the **Package Settings** branch.
8. The **Package Settings > Base Package** field shows the **Name**, **Version** and an optional **Description** field for the **Base** package to be deployed.
9. If you need to add an updated package or the packages are not stored in the default location, click **Select**.
   - The **Manage Packages** window opens.
   - The Endpoint Security Management Console window shows the available default packages. Select a provided package and click **OK**.
   - 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**.
For example, to install the Initial Package (the minimal client that can later retrieve and install Software Blades), select `Master_MIN.EPS.msi`

If you want to add a Check Point Hotfix or HFA (Hotfix Accumulator package), click Add. The Manage Packages window opens. Click Import to browse to the Check Point package and then click OK.

The HFA and Hotfixes field shows available HFAs and Hotfix packages that can be added to the profile.

10. Click OK.

Continue with following procedures to add Authentication Settings, Signature, and VPN site definition to the client installation, or with configuration of the initial package.

Global Package Configurations

Configure up the global settings for all client packages before you create specific packages.

To set up global package configurations:

- Open Software Deployment > Overview.
- If the Global Packages Configurations and Content pane is not visible, select this command from the View menu.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working in unauthenticated mode</td>
<td>Any machine with an Endpoint Security client installed can connect to the server. To provide more security, enable Authentication Mode.</td>
<td>Configuring Authentication (on page 40)</td>
</tr>
<tr>
<td>Domains with strong authentication</td>
<td>Listed Active Directory domains are configured for Strong Authentication; this cannot be reversed.</td>
<td></td>
</tr>
<tr>
<td>Packages signed by CA</td>
<td>Client packages may be signed by the Certificate Authority; connection between clients and server is trusted</td>
<td>Providing Software Signatures (on page 38)</td>
</tr>
<tr>
<td>VPN sites defined</td>
<td>Client packages may include a default VPN connection setting</td>
<td>Configuring VPN Client Settings (on page 38)</td>
</tr>
</tbody>
</table>

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 have VPN capabilities, with the Check Point Endpoint Connect VPN client an enabled feature.

**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. Open Software Deployment > VPN Client Settings.
2. Click New.
   - The Endpoint Secure Configuration window opens.
3. Provide the VPN Site details.
Configuring Client Packages

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Provide 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>Provide 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.</td>
</tr>
</tbody>
</table>

<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>

Configuring VPN Client Settings

You can override the default VPN client settings for a client package and configure the package to use a VPN site that you select.

To create VPN client settings for a package:

2. Select the relevant profile, and click the Export Package button. A message displays asking you to enter the uninstall password.
3. Enter the uninstall password, and click OK.
4. A message displays asking you if you want to override the default VPN client settings configuration.
5. Click Yes.
6. The VPN Client Settings window opens.
7. If you are using Endpoint Connect, do the following:
   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. For information on creating a VPN site, see Providing Default VPN Configuration.
      (ii) If you select Import from file, browse to the configuration file you want to use, and click OK.
8. If you are using Secure Client, do the following:
   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.

Providing Software Signatures

You can ensure that remote endpoints of your organization receive the correct MSI package by adding a signature to the client package. The certificate is held on the server and authenticated by the endpoints. By default, an internal signature is created.
To create a custom signature:
1. Open Software Deployment > Software Signature.
2. In the Certificate Settings options, select Custom.
3. Browse to the certificate (P12 file) to use.
4. Provide a password.
   The certificate is created on the Endpoint Security Management Server. Copy this file and send to client machines before installing the client.

Understanding Endpoint Security Authentication

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

The system can function in different modes:

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

- **Strong Authentication** mode - Each connecting computer and the user working on it are authenticated with the Endpoint Security Management Server, using industry-standard Kerberos protection through the Active Directory server.

**Figure 5-1**  Endpoint Security Authentication Process

The authentication process:

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

The default behavior after Security Management Server installation is Unauthenticated mode. It is recommended that you use this mode while you are evaluating Endpoint Security, in a lab environment; and that you switch to Strong Authentication just before moving to a production environment. It is not recommended to continue to work in Unauthenticated mode after moving to production in a live environment.

**Important** - As soon as you configure your Endpoint Security Management Server to work with only authenticated clients, you cannot reverse the setting. Any machine on which the client agent is installed, but which does not belong to an Active Directory, will not be included in Endpoint Security management.
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:
2. Make sure all the clients and the Endpoint Security Management Server are in the Active Directory.
3. Configure Access Zones, Application Control, and other Software Blade configurations that you want to include in policies.
4. Monitor for undesired activity and modify configurations as needed.
   For example, change configurations if legitimate traffic is blocked or if Anti-malware reports show a need for more security.
5. When you are ready to move to a production environment, map the Kerberos service to a Domain user ("Configuring Active Directory for Authentication" on page 42).
7. Configure a new Endpoint Security client package with the Authentication profile ("Exporting Packages" on page 41).
8. Deploy the client MSI ("Handling Client Packages" on page 44).

Troubleshooting Authentication

Check the Authentication log in %uepmdir%/logs\Authentication.log.

If the Authentication.log file on the client shows:

Credentials acquired for server@REALM.COM
Message is Empty.
Security context is not yet established. continue needed.

- Check that the client is in the domain for of the packaged authentication principles, and that it can connect to the Domain Controller.
- Check the service name for typing or formatting errors. If there is an error, correct it in the Endpoint Security Management Console, create a new client package, and restart the client.

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. Re-do the process to configure authentication ("Configuring Authentication" on page 40).

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 machines 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
Configuring Client Packages

Installing and Deploying Endpoint Security Clients

%UEPMDIR%\endine\conf\global.properties, add this line:
authentication.clockSkew.secs=<seconds>, where you replace <seconds> with the clock skew in seconds that you want to allow.

Exporting Packages

After you have selected the client MSI and configured its settings, export the client package.

To Export a client package:
1. Open Software Deployment
2. View by: Profiles.
3. Click Export Packages.
   The Uninstall Password window opens.
4. Enter the password needed to uninstall the client.
5. Click OK.
   The Browse For Folder window opens.
6. Select the location to save the new client installer MSI.
7. Wait until a message opens: Generating msi file complete.

Configuring and Installing Initial Package

If this is the first client package installed on the endpoint, you must configure it to communicate with the Endpoint Security Management Server.

This is done only for the initial client packages - or if you need to change the server IP address or authentication configuration. Subsequent client package modifications, such as adding Software Blades, are done with the Install Policies command. The upgraded packages retain the server IP address that you configured for the initial client.

To configure the initial client package:
1. Open the %FWDIR%\conf\smc_files\uepm\DA\config.dat file.
   This file is created after Export.
2. Check that the IP address of the Endpoint Security Management Server is correctly provided. If you need to change it, Export again.
3. Use GPO, SMS, email with shared network path, or another distribution method to deploy the initial client package to endpoints.

   When the client is installed on an endpoint, it contacts with the Endpoint Security Management Server. Check the Endpoint Status report in the Monitoring tab, to monitor connection issues.

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.

<table>
<thead>
<tr>
<th>Blade or Feature</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Features</td>
<td>• Firewall Rules</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Compliance</td>
</tr>
<tr>
<td></td>
<td>• Application Control</td>
</tr>
<tr>
<td></td>
<td>• Malware Protection</td>
</tr>
<tr>
<td></td>
<td>All function the same as in the full production client but using the default policies.</td>
</tr>
</tbody>
</table>
Configuring Client Packages

### Full Disk Encryption

During the installation, you have to decide between:

- Encrypt all disks with a fixed key
- Do not encrypt any disk

If you decide to encrypt, the hard drive is encrypted using AES 236-bit for 15 days. After 15 days evaluation, the disk decrypts.

If you need to recover ("Full Disk Encryption Recovery" on page 69) 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

Functions the same as in the production client. Licenses are enforced by the gateway.

### WebCheck

Functions 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.

---

### Configuring Active Directory for Authentication


#### To Prepare the Active Directory Server for Authentication:

1. Run **suptools.msi** to install the Windows Server 2003 Support Tools package.
2. Run **ktpass.exe**.
3. Open **Microsoft > Active Directory Console - Users and Computers**.
4. Create a domain user and clear the **User must change password at next logon** option.
5. Run this command to map a service to a user:

   Syntax:
   
   ```
   ktpass princ ServiceName/realm@REALM mapuser <userName>@REALM pass <userPass> out <name of outFile>
   ```

   **Example**:
   
   ```
   ktpass princ tst/nac1.com@NAC1.COM mapuser auth-user@NAC1.COM pass 123456 out outfile.keytab
   ```

   Where:
   
   - **ServiceName** = **tst**
   - **realm** (domain name) = **NAC1.COM** (in princ command: the first time in lower case and the second in upper case)
   - **userName** = **auth-user** (user from item 4)
   - **userPass** = **123456** (password for user from item 4)
   - **name of outFile** = **outfile.keytab** = encrypted keytab file
6. Save the console output to a text file. See the version number (vno) and encryption type (etype).

Sample output:
Targeting domain controller: nac1-dc.nac1.com
Successfully mapped tst/nac1.com to auth-user.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to outfile.log:
Keytab version: 0x502
keysize 74 tst/nac1.com@NAC1.COM ptype 0 (KRB5_NT_UNKNOWN) vno 7 etype 0x17 (RC4-HMAC) keylength 16 (0x32ed87bdbc5e9cbea88547376818d4)

Windows 7 Clients and Ktpass
If you are using a ktpass older than version 5.2.3790.1830, ARC4-HMAC encryption might not be available and the resulting default encryption method based on DES. DES is not considered a safe encryption method. By default, Windows 7 does use DES encryption, and this can create issues with Windows 7 clients. For this reason, Check Point recommends downloading the latest version of ktpass.exe that is compatible with your Windows server and supports ARC4-HMAC encryption. If you still need clients on Windows 7 to authenticate using DES:

1. Log in to the Windows 7 client with administrator credentials.
2. Start > Run > gpedit.msc.
3. Browse to:
   Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.
5. Select DES_CBC_MDC.
6. Click OK.

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. Provide the details of the configured Active Directory, taken from the output of the Active Directory map service command.

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

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket encryption method</td>
<td>Select the encryption method according to the Active Directory output.</td>
</tr>
<tr>
<td>Key version number</td>
<td>Provide the version number according to the Active Directory output.</td>
</tr>
</tbody>
</table>

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

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

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

It will take time for the clients and the Endpoint Security Management Server to synchronize. During this time, the environment will remain unauthenticated, and some operations will fail. The exact amount of time depends on the synchronization interval ("Directory Synchronization" on page 21).

### Deploying Subsequent Client Packages

After endpoints have the initial client installed, and have made contact with the Endpoint Security Management Server, you can modify the client, usually to upgrade it with more Software Blades.

**To deploy clients after the initial client is installed:**

1. Configure the policy that this client will use.
2. Create the package.
3. From the **File** menu, click **Install Policies**

### Handling Client Packages

The **Software Deployment** tab > **Packages** pane, is your repository of available Endpoint Security client packages (MSI files).

If you have another MSI file to install Endpoint Security clients, you can add them here: click **Add from file** and then browse to the MSI file.

When the client package is ready to deploy on endpoint machines, you can distribute the package using GPO or another third-party distribution method. All Endpoint Security client packages are created for silent network installation on endpoints.
Chapter 6

Upgrading Clients

This section covers client upgrades.

In This Chapter

Upgrading to R80.10 Clients 45
Upgrading Legacy Clients 45

Upgrading to R80.10 Clients

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

- DA and blades are upgraded together. You cannot upgrade only the DA.
- The upgraded 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.

How clients are upgraded:

1. You configure Software Deployment and install the policy.
2. The DA downloads the new package.
   - If the Software Deployment policy is configured for silent restart, the DA starts the installation. Then it reboots the computer immediately, without user notification.
   - Otherwise, the DA sends a message to the user: 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 installation to start now? If you choose No, installation will start automatically at HH:MM. The message opens again at ten-minute intervals.
3. The DA installs the new client.
   - Installation starts automatically after a timeout if the user did not click Yes. You can configure the message interval and the timeout in the Common Client Policy > General Properties > Client Install / Uninstall Settings.
4. After installation, the DA reboots the computer.

Upgrading Legacy Clients

Only R71 clients (and higher) can be successfully upgraded to R80.10 offline and online.

- Offline - The endpoint has no connection with the Endpoint Security Management server.
- Online - The endpoint can connect with the server.
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 R80.10 client with the necessary blades and policies

To create an offline upgrade package:
1. On Software Deployment tab, click New.
2. The Software Deployment Profile window opens.
3. Create a profile with the needed blades.
4. Click OK.
5. Select the new profile in the table, and click Export Package.
   The Uninstall Password window opens.
6. In the Legacy Upgrade area, select Support legacy upgrade and enter the passwords needed to uninstall legacy products.
7. In the FDE Update Validation Password area, select Support legacy upgrade and enter the passwords needed before the legacy Full Disk Encryption can be upgraded to the latest version.
8. Click OK.
9. The packet exports to the chosen directory.
10. Supply the EPS.msi file to the offline endpoints on the network.

Online Upgrades

During an online upgrade the endpoint has a connection to the server and downloads an initial client (the Endpoint Security Agent). The initial agent uses the Common Client Policy that contains uninstall passwords for legacy products.

To create a package for Online upgrade:
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
5. Click OK.
7. The Uninstall Password window opens giving you a chance to change the uninstall passwords.
8. Click OK.
9. Browse to a folder and save the Endpoint Security Agent package.
10. Deploy the client package to endpoints.
Chapter 7

Managing Policies and Users

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

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

In This Chapter

- About Policies 47
- Assigning Policies 50
- Deploying Policies 53

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>Endpoint Compliance</td>
<td>Ensures that protected computers comply with your organization's requirements, and allows you to assign different security levels according to compliance state. For example, non-compliance may result in a remediation message, a warning, or restriction from the network.</td>
</tr>
<tr>
<td>WebCheck</td>
<td>Protects endpoint computers against phishing - websites impersonating other websites for malicious purposes.</td>
</tr>
<tr>
<td>Common Client Settings</td>
<td>Defines a common policy for multiple endpoint clients. This lets you deploy and maintain many clients efficiently.</td>
</tr>
</tbody>
</table>
State of Compliance

Policy settings may determine what applications can be installed or executed on a computer, what must be installed or running, and what is not allowed.

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 consists of a set of compliance rules. If the user is in violation of a compliance rule, then the policy specifies the compliance action that should be taken by the client, namely ‘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.

The alert can be configured by the administrator in the management console. The administrator can specify different alert messages (in different languages) for different states if required, such as:

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

The administrator can choose to configure the policy to auto-remediate if the endpoint is non-compliant. Action is taken either by clicking the remediation link in the client's alert window, or via auto-remediation where a tooltip can be configured to display a message in the Endpoint Security tray icon, i.e., “Remediation in progress”.

Connected, Disconnected or Restricted

When you assign a policy to computers or users, you choose that the policy be assigned for:

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

The Connected Policy is the configuration that is enforced when the endpoint computer is connected to the Endpoint Security Management Server (either when it is physically located on the Office LAN or through a
RemoteAccess connection). This policy is used not only to protect the endpoint computer from threats, but also to protect other computers on your network and to enforce your corporate policy.

The **Disconnected Policy** is enforced when the endpoint computer is not connected to the Endpoint Security Management Server. For example, you may want this policy to be more restrictive to protect computers when their users are working from home and are not protected by the organizational resources.

The **Restricted Policy** is enforced when an endpoint computer, in either a connected or disconnected state is out-of-compliance with a deployed Media Encryption & Port Protection, Firewall Rules or Application Control policy, or policies for a pre-configured number of heartbeats. Since the Endpoint Agent performs the heartbeats and is aware of compliance status, it is the component which establishes restricted mode.

The client enforces Security Policies associated with restricted mode, if any, and reports restricted mode to the server.

**How Connected, Disconnected, and Restricted Policies are Assigned**

When an endpoint is connected to the Endpoint Security Management Server, the endpoint gets the policy assignment according to the organizational hierarchy and direct assignments.

- When an endpoint is disconnected from the Endpoint Security Management Server, the endpoint uses its User Disconnected Policy assignment. If it does not have a Disconnected assignment, it uses its default (Connected) policy.
- Endpoints that are non-compliant for a configured number of heartbeats switch over to the current user Restricted Policy and remain there until they become compliant. After compliance, endpoints return to the policy assigned to them prior to becoming non-compliant.

**Configuring Connected, Disconnected or Restricted State**

**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.

   The Disconnected policy is assigned to the node for use when it is not connected to the corporate network.

**To set an assigned policy to 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. Click Add Policy When > Restricted.
4. Click Install Policy.

   The Restricted policy will be assigned to the node if it becomes non-compliant with a policy or policies assigned to it. Note that the Restricted state can be applied only to these policies:

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

**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.
User Policy or Machine Policy

Some configurations are defined in the context of a certain User, while others are defined for a certain Machine. 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 machine they choose to use.

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

Configuring the Heartbeat Interval

Compliance check settings are regulated by the number of heartbeats. The heartbeat interval can be adjusted.

*Note* - Setting an extremely low heartbeat interval can result in performance issues. Setting an extremely high heartbeat interval can result in decreased security and less accurate reporting. The default heartbeat is set at 60 seconds.

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

Assigning Policies

For Endpoint Security clients to receive configurations, the policy containing the configurations must be assigned to the endpoints.

*Note* - Before installing the software package on an endpoint client for the first time, you must configure the policies and click Install Policies, so that they are made available for the endpoint clients.

You can assign policies to a number of nodes with clients inheriting the policy from a larger container object. For example, the My Organization node must always have the default policies assigned - there is always a Firewall Rules policy assigned to the root. This Firewall Rules policy is then inherited by all the nodes in the tree unless you assign another Firewall Rules policy to a specific node.

*Note* - This is not true if a policy has been directly assigned to the client. The direct assignment takes priority.

Direct Assignment

You can create and assign a policy to an object in the organizational tree; or you can allow a user or computer to 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 the children directories, networks, machines, 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 machines.
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

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

Precedence is set for different organizational entities:

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

Group Assignment Priority

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

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

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

- Global Group Priority Assignment
- Blade Priority Assignment

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

To Set the Global Group Assignment Priority:

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

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

The **Global: Group Assignment Priority** window opens.
6. Use the arrow buttons to move a group up or down.
7. Click **OK**. The group at the top of the list gets the highest priority.

For example:

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

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

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

The Group Assignment Priority window for the blade shows two options.
- Use global group assignment priority to inherit the global priority (default)
- Override global group assignment priority to override the global priority
7. Select Override global group assignment priority.
8. Use the arrow buttons to reorder the groups.
9. Click OK.
   The group at the top of the list gets the highest priority.
   For example:
   - John belongs to two AD Groups, PR and Sales.
   - The two groups have the Malware Protection blade enabled.
   - The PR groups' Malware Protection blade has a High Security Policy.
   - The Sales group has a Low Security policy.
   - Group Assignment Priority has Sales above PR in the list.
   Based on Group Assignment Priority, John's Malware Protection blade receives the Low security policy.

Recommendations for Management

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

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

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

<table>
<thead>
<tr>
<th>Container Object</th>
<th>Assignment Description</th>
</tr>
</thead>
</table>
| 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. |
## Container Object | Assignment Description
--- | ---
Organizational Units | Assign a policy to OUs to have the policy apply to users and machines belonging to the OU.
Groups | Assign a policy to User or Computer groups that were already defined in the active directory.
If you assign a policy to an Active Directory group, a node may belong to more than one group, and therefore it will enforce the policy of the highest ranking group to which it belongs.
IP Network Range | Use this group to enforce security according to the location of the endpoint, regardless of placement in the active directory. For example, you can use IP Network Ranges to create different policies for users when connecting through your VPN.
**Note:** If your organization and endpoints will use a VPN, assign a policy to the Security Gateway to ensure that users have the appropriate access.
Individual endpoint users | Assign a policy directly to one or more users to provide exceptions to your general security practices.
Individual endpoint computers | Assign a policy directly to one or more computers to provide exceptions to your general security practices.

### Viewing Assignments

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

**To view policy assignments:**

1. On the Policies tab, select a blade.
   - The **Overview** page for that blade shows
2. In the **View by** box, select **Assignment**.
   - The console shows each node that has this policy
3. Click **Overview** in the tree.
4. The **Policy Overview** page shows:
   - **Policy Assignment per blade**, a way of seeing how many policies are in use
   - **Policy Status**, which 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.
Chapter 8

OneCheck Settings Policies

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

OneCheck Settings define:

- How users should authenticate themselves to Endpoint Security.
- If users should be allowed direct access Windows once they have become authenticated to Endpoint Security without having to log on to Windows, too.
- A time limit for how long a user is to be allowed access to a computer, and what should happen if the user enters invalid authentication details.
- If Remote Help is to be allowed, so that users will be able to receive help from an administrator, for example if their computers become locked due to too many failed authentication attempts.

Note - Single Sign On is always enabled when using OneCheck Settings.

In This Chapter

Quick Start 54
Viewing OneCheck User Settings Policy Assignments 55
OneCheck Logon Assignments 55
Properties for OneCheck User Settings 55
Account Lockout 56
Password Security 56
Password Security - Custom Level 56
Permissions 57
Role-Based Administration 58

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:

1. On the Endpoint Security Management Server console, open the **Policies** tab and select **OneCheck User Settings Policies** on the **Navigation** tree.
   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.
6. Click **OK**.
The assignment is shown on the Assignment window.

7. Click OK.

Viewing OneCheck User Settings Policy Assignments

You can view 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 Logon Assignments

To assign a policy:
1. On the Compliance Rules Policy Overview page, open an existing policy or create a new one.
3. Click Assignment in the navigation tree.
4. Click Add Assignment.
5. Click Connected to enterprise.
   The Select Node window opens.
6. In the Navigation Tree, select a node in the directory. When selecting a directory or group, users belonging to that group or directory show in the Node area.
7. Click OK.
8. On the Assignment page, click the Add Assignment down arrow, and select from the displayed options.
9. Click OK.
10. Click Save & Install.

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 Save & Install.

Properties for OneCheck User Settings

There are a number of properties 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 machine. To remedy the situation, the user will have to receive Remote Help from an administrator.</td>
</tr>
<tr>
<td>Number of failed attempts before a temporary lockout</td>
<td>The maximum number of failed logon attempts allowed before the user account is temporarily locked out from the machine for a defined duration.</td>
</tr>
<tr>
<td>Duration of a temporary lockout</td>
<td>If the temporary lockout option is selected, this sets the duration of a temporary lockout, in number of minutes.</td>
</tr>
<tr>
<td>Maximum number of successful logons allowed before the account is locked</td>
<td>The maximum number of times that a user can log on to Endpoint Security. When this is reached, the user account cannot be used. To unlock an account, you must disable this feature in the active policy or increase this value for the policy. Remote Help cannot be used.</td>
</tr>
</tbody>
</table>

# Password Security

Use these settings to set required security parameters for passwords. 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.
### 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>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>
<tr>
<td>Use custom requirements</td>
<td>If you select this, select the requirements for which type of characters the password must contain or not contain:</td>
</tr>
<tr>
<td></td>
<td>• Consecutive identical characters, for example, aa or 33</td>
</tr>
<tr>
<td></td>
<td>• Require special characters. These can be: ! &quot; # $ % &amp; ' ( ) * + , - . / : &lt; = &gt; ? @ {</td>
</tr>
<tr>
<td></td>
<td>• Require digits, for example 8 or 4.</td>
</tr>
<tr>
<td></td>
<td>• Require lower case characters, for example g or t.</td>
</tr>
<tr>
<td></td>
<td>• Require upper case characters, for example F or G.</td>
</tr>
<tr>
<td></td>
<td>• Password must not contain user name or full name.</td>
</tr>
<tr>
<td>Minimum length of password</td>
<td>Enter the minimum number of characters for a valid password.</td>
</tr>
<tr>
<td>Password can be changed only after</td>
<td>Enter the minimum number of days that a password must be valid before the user can change it.</td>
</tr>
<tr>
<td>Password expires after</td>
<td>Enter the maximum number of days that a password can be valid before the user must change it.</td>
</tr>
<tr>
<td>Number of passwords</td>
<td>Enter the minimum number of password changes needed before a previously used password can be used again.</td>
</tr>
</tbody>
</table>

### Permissions

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow logon to system hibernated by another user</td>
<td>Lets a different user than the logged on user authenticate in preboot to a system in hibernate mode.</td>
</tr>
<tr>
<td>Allow user of recovery media</td>
<td>Let user authenticate to use recovery media to recover and decrypt data from an encrypted system.</td>
</tr>
<tr>
<td>Allow user to change his credentials from the endpoint client</td>
<td>Let users change the password on an endpoint client during the Preboot.</td>
</tr>
<tr>
<td>Allow Single Sign-On use</td>
<td>Let users use Single Sign On to log on to Preboot and Windows when OneCheck Logon is disabled. Single Sign on applies only to Preboot and Windows and not to different blades, such as VPN or Media Encryption. Users are always allowed to use Single Sign On when OneCheck Logon is running.</td>
</tr>
<tr>
<td>Allow account to receive remote password change help</td>
<td>Remote password change help is for users who use a fixed password, a one-time password card. Let the user get help from an administrator to reset the account password (for example, if the user forgets the password).</td>
</tr>
</tbody>
</table>
Role-Based Administration

Administrator roles determine Read/Write permissions, policy installation, and Remote Help access in Endpoint Security.

You must have Read/Write All and Manage Administrator permissions to define and revise these administrator roles:

- **Full Access** - Administrators with Read/Write All permissions. The administrator has permissions to edit the object database, install policies, and access Remote Help.
- **Read-Only** - Auditors with Read-Only permissions. Save and Install buttons are disabled. The administrator can be assigned Remote Help access by an administrator with management permissions.
- **Help Desk** - Administrators with Read/Write permissions. The administrator can be assigned Install Policies and Remote Help access permissions.
- **Remote Help** - Administrator can view only the Endpoint Security Management Server Console Overview page for Remote Help access.

To assign an Endpoint Security administrator role:

2. Click Manage > Users and Administrators. The Users and Administrators window appears.
4. Enter the administrator login name and click New to assign the permissions profile. The Permissions Profile window appears.
5. Enter the administrator name.
6. In the Permissions area, select Customized and click Edit.
7. On the General tab, select Endpoint Security and Read/Write or Read-Only.
8. On the Endpoint Security tab, select the administrator role.
9. Click OK.
10. The Administration Properties window shows the permission profile for the administrator. Click OK.

**Note** - On the Administration Properties window, click View Profile to display the administrator’s profile settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 9

Endpoint Security Licensing

This chapter covers licensing in Endpoint Security.

In This Chapter

- Evaluation Mode License 59
- Product License 59
- Plug and Play License 59

Evaluation Mode License

- The Evaluation Mode demo license is on request only. The 30 day license is for specified software blades. A message to update the license appears on the client in the Full Disk Encryption row of the Software Blades area, seven days prior to expiration. At license expiration, the client is automatically decrypted.

- On the server side, the evaluation license covers the number of seats and time period as defined in the evaluation agreement reached with Check Point.

Product License

- Endpoint Security software blades can be updated from Plug and Play or Evaluation Mode licenses to a Product license.

- A Product license must be purchased for each of the software blades in use, as well as other Endpoint Security components running on the client.

- Product licenses are installed on the server through SmartUpdate.

- If the Full Disk Encryption Product license expires ("Full Disk Encryption Licenses" on page 70), the client is automatically decrypted.

Plug and Play License

- Plug and Play is a 15 day demo license that is automatically installed with Endpoint Security software and can be upgraded to a full production license.

- The Plug and Play license provides use of all Endpoint Security software blades for a 100 seats.

- After the Plug and Play license expires, the client is not automatically decrypted.
Chapter 10

Full Disk Encryption

Full Disk Encryption protects stored data on computer disks from illegal access. When the disk is turned off, in sleep or hibernation mode, data sector-by-sector encryption protects the data. Full Disk Encryption:

- Ensures computers use strong user authentication
- Locks user accounts after too many failed login attempts.

In This Chapter

Quick Start 60
Viewing Full Disk Encryption Policy Assignments 61
Creating a Customized Full Disk Encryption Policy 61
Full Disk Encryption Installation and Deployment 68
Full Disk Encryption Recovery 69
Upgrading to Check Point Endpoint Security 70
Full Disk Encryption Licenses 70
Full Disk Encryption Troubleshooting 70

Quick Start

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

To Quickly Assign a Predefined Policy:
1. On the Endpoint Security Management Server 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 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.
Viewing Full Disk Encryption Policy Assignments

One or more Policies can be attached to all of the 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 61)
   - Preboot Protection (on page 62)
   - User Acquisition (on page 66)
   - OneCheck ("OneCheck Logon" on page 67)
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 |
Creating a Customized Full Disk Encryption Policy

### Security Level

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 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 Windows Integrated Logon and Wake On LAN based on your environment.

### Security Level

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning:</th>
</tr>
</thead>
</table>
| Custom               | • Wake On LAN disabled after two failed logon attempts  
                        | • Endpoint disables Wake On LAN after 65 days  
                        | • Windows Integrated Logon disabled after 9 failed logon attempts to Windows  
                        | • Remote Help enabled  
                        | • Hardware Hash enabled  
                        | **Note**: these default settings can be adjusted. |
| Low User Trust       | • Wake On LAN disabled after two failed logon attempts  
                        | • Endpoint disables Wake On LAN after 65 days  
                        | • Windows Integrated Logon disabled after 9 failed logon attempts to Windows  
                        | • Remote Help enabled  
<pre><code>                    | • Hardware Hash enabled |
</code></pre>
<table>
<thead>
<tr>
<th>Security Level</th>
<th>Meaning:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Medium User Trust</strong></td>
<td>• Wake On LAN disabled</td>
</tr>
<tr>
<td></td>
<td>• Endpoint disables Wake On LAN after 45 days</td>
</tr>
<tr>
<td></td>
<td>• Windows Integrated Logon disabled after 5 failed logon attempts to</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>• Remote Help enabled</td>
</tr>
<tr>
<td></td>
<td>• Hardware Hash enabled</td>
</tr>
<tr>
<td><strong>Higher User Trust</strong></td>
<td>• Wake On LAN disabled</td>
</tr>
<tr>
<td></td>
<td>• Endpoint disables Wake On LAN after 30 days</td>
</tr>
<tr>
<td></td>
<td>• Windows Integrated Logon disabled after 5 failed logon attempts to</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>• Remote Help enabled</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Permission</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable USB device in preboot environment</td>
<td>Select to use a device that connects to a USB port. If you use a USB Smart Card you must have this enabled. If you do not use USB Smart Cards, you might need this enabled to use a mouse and keyboard during Preboot.</td>
</tr>
<tr>
<td>Enable mouse in preboot environment</td>
<td>Select to use a configured, driver-installed mouse to input authentication in the Preboot environment.</td>
</tr>
<tr>
<td>Allow Serial Over LAN in preboot environment</td>
<td>Serial over LAN requires an Intel vPro-enabled PC and a telnet session to the client. This option lets administrators log onto the Preboot environment remotely.</td>
</tr>
<tr>
<td>Allow graphics mode in preboot</td>
<td>Select to display the Preboot environment in low-resource mode.</td>
</tr>
<tr>
<td>Maximum number of failed logons allowed before reboot</td>
<td>• If active, specify the maximum number of failed logons allowed before a reboot takes place.</td>
</tr>
<tr>
<td></td>
<td>• This setting does not apply to smart cards. Smartcards have their own thresholds for failed logons.</td>
</tr>
<tr>
<td>Verification text for a successful logon will be displayed for</td>
<td>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.</td>
</tr>
<tr>
<td>Allow hibernation and crash dumps</td>
<td>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. <strong>Note</strong>: 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.</td>
</tr>
</tbody>
</table>

**Note** - Users assigned to a higher level node in the AD who have permission to log into a preboot environment maybe 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 machine.
3. Click **Configure** for more granular control over:
   - Windows Integrated Logon (on page 64)
   - Wake On LAN (on page 65)
   - Remote Help (on page 65)

**Windows Integrated Logon**

Although not recommended by Check Point, Windows Integrated Logon lets the administrator bypass Preboot protection. However, these settings can be overridden on the client. ("Overriding Preboot Settings" on page 66)

When implementing Windows Integrated Logon, weigh the cost of implementing Pre-Boot Authentication against the necessity for strong security while accessing the encrypted data. Windows Integrated Logon simplifies the user's experience when logging on to encrypted drives at the cost of limiting the strength of the computer's security configuration. As an alternative to Windows Integrated Logon, consider Single Sign-On (SSO) in conjunction with proper Preboot Authentication.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic logon to bypass Preboot authentication at installation</td>
<td>Switches on Windows Integrated Logon.</td>
</tr>
<tr>
<td>Maximum failed logons in Windows before Windows Integrated Logon is disabled</td>
<td>If the number of failed logon attempts exceeds the number of tries specified, Windows Integrated Logon 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, Windows Integrated Logon 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, Windows Integrated Logon 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 Windows Integrated Logon will be disabled. The computer reboots automatically, and the user must authenticate in Preboot. <strong>Warning:</strong> Disable Windows Integrated Logon 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>WIL failure Preboot message</td>
<td>Enter a message to display to the user if Windows Integrated Logon 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 Windows Integrated Logon is disabled. The computer reboots automatically and the user must authenticate in Preboot. If one IP address replies, Windows Integrated Logon 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 Windows Integrated Logon if the event fails.

If you lower the security by using Windows Integrated Logon to bypass the Preboot, 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 Windows Integrated Logon is disabled

Wake On LAN

Wake On LAN lets the administrator bypass Preboot protection for maintenance. However, these settings can be overridden on the client. ("Overriding Preboot Settings" on page 66)

Wake On LAN is a network standard that activates a computer by sending a network message. Although Full Disk Encryption Wake On LAN is frequently used in conjunction with a Wake On LAN supported network card, such a card is not necessary.

To configure Wake On LAN:

2. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Wake-On-Lan</td>
<td>Switches on Wake On LAN</td>
</tr>
<tr>
<td>The Endpoint disables Wake-On-LAN after (automatic logons)</td>
<td>Enter the number of times the Wake On LAN functionality can be used. After the number of logons expires, Wake On LAN is disabled on the client and the Preboot environment shows.</td>
</tr>
<tr>
<td>The Endpoint disables Wake-On-LAN after (days)</td>
<td>Enter the number of days for which Wake On LAN functionality is enabled. After the number of days expires, Wake On LAN 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 (minutes)</td>
<td>Enter the time delay in minutes. After the delay expires, Wake On LAN 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 to log in to Windows after the Wake On LAN logon.</td>
</tr>
</tbody>
</table>

Notes -

- Dynamic events on the client, such as a Network Location Awareness Verification, disable Wake On LAN if the event fails.
- Wake On LAN 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 Wake On LAN 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.

**Overriding Preboot Settings**

Windows Integrated Logon, Wake On LAN, and Remote Help policy settings can be overridden for specified Endpoint clients.

**To override Preboot Settings:**
1. In the Endpoint Security Management Console, open the My Organization tab.
2. Select a user's machine.
3. Right-click, and select Computer Details.
The Computer Details window opens.
4. Select User Logon Preboot Settings.

Use the options to:
- Enable Windows Integrated Logon or Wake On LAN separately or together.
- Disable Windows Integrated Logon or Wake On LAN together.
- Add or remove users approved to log on to the user's machine.

**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 replaces the logon window for:

- Full Disk Encryption
- Media Encryption & Port Protection
- Windows
- VPN

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. If you do not enter
text after enabling the screensaver, a Full Disk Encryption policy is not downloaded to the client.

Policy Assignment

To assign a policy:

1. On the Compliance Rules Policy Overview page, open an existing policy or create a new one.
3. Click **Assignment** in the navigation tree.
4. Click **Add Assignment**.
5. Click **Connected to enterprise**.
   
   The Select Node window opens.
6. In the Navigation Tree, select a node in the directory. When selecting a directory or group, users
   belonging to that group or directory show in the **Node** area.
7. Click **OK**.
8. On the Assignment page, click the **Add Assignment** down arrow, and select from the displayed
   options.
9. Click **OK**.
10. Click **Save & Install**.

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**.

Click **Save & Install**.
Full Disk Encryption Installation and Deployment

Full Disk Encryption Deployment mode refers to the period of time during which the following occurs:

- Installation of the Full Disk Encryption software blade
- Download and enforcement of the Full Disk Encryption policy

After the client is installed, Endpoint Security automatically deploys the Full Disk Encryption policy. The policy is defined in the Full Disk Encryption Policy and OneCheck Policy window on the Policies tab of the Endpoint Security Management Console:

Policies tab > Full Disk Encryption > Full Disk Encryption Overview Policy.

Full Disk Encryption policies are stored on the Unified Endpoint Management database and replicated to the Endpoint Security Management Server.

Client Requirements for Full Disk Encryption Deployment

- Full Disk Encryption blade enabled on the client
- 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.

Deployment Mode Process

Steps in the Full Disk Encryption Deployment Mode that are automatically implemented:

1. Download Full Disk Encryption policies from the server.
2. Run User Acquisition (on page 66), according to Full Disk Encryption policies.
3. Make sure that at least one user is assigned rights to log on and to run recovery media ("Full Disk Encryption Recovery" on page 69).
4. Implement Windows Integrated Logon (on page 64) or Wake-on-LAN ("Wake On LAN" on page 65), if selected.
5. Implement Remote Help.
6. Create all required system areas and update all required boot records ("Preboot Protection" on page 62), according to the Full Disk Encryption policies.
7. Supply recovery data ("Full Disk Encryption Recovery" on page 69) to the server.
8. Activate Preboot, and update boot record on boot volume.

On the Endpoint Security server, the Full Disk Encryption deployment status is displayed in the Installed Modules window.

Minimal Deployment Mode Configuration

Full Disk Encryption cannot start unless:

- At least one user assigned to the client must have Allow Use for Recovery Media permission, located on the Policies tab below OneCheck User Settings Policy > Advanced > Permissions.
- User Acquisition is enabled and has at least one user from the Microsoft Windows Active Directory with permission to log into Windows.
- Communication exists between the Endpoint Security Management Server and the client.

Note - A reboot is required to make sure Preboot is running before starting the encryption and to validate authentication credentials.
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>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 machine, the disk can be decrypted and the data recovered using Full Disk Encryption Recovery Media. Full Disk Encryption Recovery Media lets a user decrypt a disk and restore the initial boot records.

Note - Only users with Recovery permissions can restore data from the client.

To Give Recovery Permission:
1. In the Endpoint Security Management Console, open OneCheck User Settings Policy.
2. Open a policy for editing.
3. On the Advanced > Permissions page, select Allow use of recovery media.
   
   Recovery Media:
   - Is a snapshot of a subset of the Full Disk Encryption database on the client
   - Contains only the data required to do the recovery
   - Updates if more volumes are encrypted or decrypted
   - Removes only encryption from the disk and boot protection
   - Does not remove Windows components

To set up data recovery:
1. In the Endpoint Security Management Console, open My Organization.
2. Double-click a folder from the navigation tree to see the users and machines that it contains.
3. Right-click the machine 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. Select a destination for the Recovery Media:
   - For a bootable CD/DVD, enter a path to a directory for the ISO file.
   - For a USB flash drive, select the target drive from the list.
   
   Note - Creating a recovery media on a USB flash disk formats the device and removes all previous content.

5. Make sure the user knows:
   - The correct user name and password.
   - How to boot the machine: by CD or USB device.
To Recover an Encrypted Disk:
1. Make sure you are using the correct Full Disk Encryption Recovery Media. If the incorrect recovery media is used, the recovery media fails to recognize volumes on the client's disks.
2. Make sure the recovery media is the most recent.
3. On the defective computer, run the recovery media from a CD/DVD or bootable USB device.
4. When the Preboot Login windows shows, enter the name and password of a user with recovery permissions.
   The disk decrypts using partition keys contained in the Recovery Media.

   **Note** - During the decryption process, the client cannot run other programs.

### Upgrading to Check Point Endpoint Security

This section describes how to upgrade from Pointsec for PC versions 6 and 7 to Check Point Endpoint Security version R80.10.

To upgrade a client, make sure that:
- Encryption (or decryption) is not running
- The Pointsec client is Version 6.3.1 or higher

Upgrade configuration details:
- The client remains encrypted during upgrade.
- All existing user and policy settings are discarded in the upgrade. Only partition keys are kept.
- The upgrade is done through the standard Endpoint Security MSI packages, which can be run manually or through Endpoint Security software deployment.

### Full Disk Encryption Licenses

Full Disk Encryption behavior depends on the Endpoint Security license assigned to the client.
- The evaluation license is not for an unlimited number of clients, but the number of clients defined in the license.
- The evaluation license is for the period defined in the license string.
- If a product license expires, the client machine does not decrypt.

### 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.

Run CPInfo if:
- Encrypting or decrypting fails on Windows.
- The selected disk or volume does not encrypt or decrypt.
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-hand pane, click Advanced.
4. Click Collect information for technical support.
   CPInfo opens at the command prompt.
5. Press ENTER to start.
   The information is collected. A window opens showing the location of the cab file.
6. Press any 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

CPInfoPreboot collects data about components in the Full Disk Encryption Preboot environment on the client.

Run CPInfoPreboot if you cannot:

- Access the Preboot Logon window.
- Log into the Preboot Logon window.
- Start encryption or decryption.

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.
To Collect Preboot Data:
1. Copy CpInfoPreboot.exe to an external media - CD, DVD, or USB device.
   - Use external media with 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.
2. Boot the client from the external media.
   
   Note: Microsoft Windows does not automatically detect USB devices after boot up. The USB device must be connected while booting to the computer.

3. Open the command prompt and type: `<path to CpInfoPreboot> <CpInfoPreboot.exe <output cap filename> <output folder name>.
   For example: C:\path\CPInfoPreboot.exe SR1234 temp.

4. CpInfoPreboot stores the output file to the designated folder.
   - If no output name is specified, the output file has the same name as the output folder.
   - If no output folder is specified, CpInfoPreboot saves the output file to the working directory on the external media. An output folder is required if the working directory is on read-only media.

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 Mode

Common Deployment Mode Issues

- User assigned to the client
- User Permission settings
- User Acquisition settings
- Volume Encryption settings
- Network communication for sending or retrieving Full Disk Encryption policy information, end-user and client settings, and supply recovery data from the server to the client.
User Acquisition

A typical installation requires user acquisition to supply user data to the server. Make sure that:

- The user has a password.
- 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 viable.
- The Driver Agent has a connection to the server.
- The Device Auxiliary Framework has a connection with the Endpoint Agent and Full Disk Encryption.

Full Disk Encryption Password and Recovery Media Rights

Make sure that at least one end-user can log into the system and run Recovery Media. If User Acquisition is not enabled, at least one user with a password must be associated with the device.

Client System Area

- To run Full Disk Encryption, the volume system area must have 32MB of free disk space.
- Disk fragmentation can affect Full Disk Encryption. Repair fragmentation by running disk defragmentation software on the volume.

Debug Logs

The Client debug log is named dlog1.txt, and found in the following places:

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

Dynamic Mount Utility

Chapter 11

Media Encryption & Port Protection Policies

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

In This Chapter

- Media Encryption & Port Protection Terminology
- Access to Media Encryption & Port Protection Policies
- Global Settings on the Overview Page
- General Properties
- Advanced Media Log
- Changing the Group Ranking Order

Media Encryption & Port Protection Terminology

- **Media Owner.** The first user to insert the media into an endpoint computer automatically becomes the **media owner.** This term applies only to users in AD environments, not workgroups.

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

Access to Media Encryption & Port Protection Policies

To access Media Encryption & Port Protection settings:

1. Click **Policies** tab > **Media Encryption & Port Protection**.
2. To:
   - Edit an existing Media Encryption & Port Protection policy, select a policy and click **Edit**.
   - 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 to 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</td>
</tr>
<tr>
<td></td>
<td>media can read and modify it, although this can be modified. Use the</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>passwords.</td>
</tr>
<tr>
<td>Media Owner Access</td>
<td>Owners of the encrypted media (the user who encrypted the content)</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>set the slider to a predefined policy or click <strong>Custom Level</strong> to open the</td>
</tr>
<tr>
<td></td>
<td><strong>Custom Device Access Settings</strong> window and create a new access policy.</td>
</tr>
<tr>
<td>Control Access to Encrypted Removable Media Devices</td>
<td>These settings are managed globally and can be found in the <strong>Policies tab &gt;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Media Encryption &amp; Port Protection</strong> node &gt; <strong>Encrypted Media Access</strong></td>
</tr>
<tr>
<td>Encrypt Removable Media</td>
<td>Configures whether removable media devices are encrypted. Click **Advanced</td>
</tr>
<tr>
<td></td>
<td><strong>Settings</strong> to configure more granular control over the process.</td>
</tr>
<tr>
<td>Scan and Authorize Removable Media</td>
<td>Select to scan devices for threats and authorize them for access. Click</td>
</tr>
<tr>
<td></td>
<td><strong>Advanced Settings</strong> to set a custom level.</td>
</tr>
</tbody>
</table>
Creating Custom Access Rules for Data

Use the Media Encryption & Port Protection Policy to set how users access non-encrypted media.

To create a custom access rule:
1. In the Media Encryption & Port Protection Policy window, select Control Access to Non-encrypted Removable Media and Peripheral Devices.
2. Click Configure.
   The Custom Device Access Settings window opens.
3. For each device row, select the access permission. For example:
   - 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.

Encrypting Removable Media

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

<table>
<thead>
<tr>
<th>Encryption Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom</td>
<td>Custom settings for removable devices</td>
</tr>
<tr>
<td>Full</td>
<td>Users can:</td>
</tr>
<tr>
<td></td>
<td>• Encrypt removable media for themselves and others</td>
</tr>
<tr>
<td></td>
<td>• Remove the encryption from the encrypted device</td>
</tr>
<tr>
<td></td>
<td>• Change the size of the existing encrypted media</td>
</tr>
<tr>
<td>Medium</td>
<td>Users can:</td>
</tr>
<tr>
<td></td>
<td>• Encrypt removable media for only themselves</td>
</tr>
<tr>
<td></td>
<td>• Change the size of the existing encrypted media</td>
</tr>
<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. Expand the Advanced Settings area to set these options:
Option | Description
--- | ---
Copy utility to media to enable media access in non-protected environments | Select to allow access to encrypted media on a client machine that does not have Endpoint Security installed. The EPM Explorer allows users working on such computers to access data on an encrypted device.

Protect media with password for read only access in offline mode | 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 allow users to recover their password using remote help to allow administrators to provide Remote Help to users who forget their passwords.

Allow users to change read only password | Lets users change their read only offline access password.

### Creating Custom Media Authorization Settings

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

To customize media authorization settings:

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automatic media authorization | Media Encryption & Port Protection triggers supported Anti-virus software, if present on the client computer, to scan removable media for viruses. If the media is clean, it is authorized and access is granted; otherwise access is blocked.
Select Allow the user to delete unauthorized files to let users to clean prohibited content from the media. |

<table>
<thead>
<tr>
<th>Manual media authorization</th>
<th>Select to provide users with greater control over media scanning.</th>
</tr>
</thead>
<tbody>
<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, devices 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.

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 12

Firewall Rules Policies

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

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

**Note** - The firewall policy is affected by Endpoint compliance states (*Non-Compliance* on page 48), and whether the Connected or Disconnected (*Connected, Disconnected or Restricted* on page 48) policy is in force.

In This Chapter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Rules Policy Options</td>
<td>79</td>
</tr>
<tr>
<td>Firewall Rules - Control Icons and Buttons</td>
<td>79</td>
</tr>
<tr>
<td>Firewall Rule Number</td>
<td>81</td>
</tr>
<tr>
<td>Creating Firewall Rules</td>
<td>82</td>
</tr>
</tbody>
</table>

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 news Network objects and services.

Firewall Rules - Control Icons and Buttons

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

<table>
<thead>
<tr>
<th>Icon/Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Rule at the</td>
<td>When adding rules to the Firewall policy, remember that rules at the top of</td>
</tr>
<tr>
<td>Bottom</td>
<td>the table are evaluated against traffic before rules at the bottom. To make</td>
</tr>
<tr>
<td></td>
<td>sure that a rule is evaluated only after all other rules have been evaluated,</td>
</tr>
<tr>
<td></td>
<td>add it to the bottom. Once the rule is located in the proper place, decide</td>
</tr>
<tr>
<td></td>
<td>whether the rule applies to inbound or outbound traffic.</td>
</tr>
<tr>
<td>Add Rule at the</td>
<td>Drag and drop rules to change the behavior of the firewall by changing the</td>
</tr>
<tr>
<td>Top</td>
<td>order in which rules are matched to traffic.</td>
</tr>
<tr>
<td>Add Rule below</td>
<td>To remove a rule, right-click the rule &gt; Delete Rule.</td>
</tr>
<tr>
<td>Current</td>
<td>(To remove a rule)</td>
</tr>
<tr>
<td>Add Rule above</td>
<td>To create a new rule (Host, Address Range, Site or Network):</td>
</tr>
<tr>
<td>Current</td>
<td>• Right-click the table heading row of General Properties &gt; New Rule&gt;</td>
</tr>
<tr>
<td></td>
<td>Inbound or Outbound. A new Inbound or Outbound rule is added at the top</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Below. The new Inbound or Outbound rule is added to the current row.</td>
</tr>
<tr>
<td>Edit</td>
<td>After modifying a firewall rule, the policy must be installed on the</td>
</tr>
<tr>
<td></td>
<td>Endpoint before it takes effect.</td>
</tr>
<tr>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Security Management Console and SmartDashboard make use of the</td>
</tr>
<tr>
<td></td>
<td>same network objects in the database. Changing an object's properties in</td>
</tr>
<tr>
<td></td>
<td>the Endpoint Security Management Console affects how the object behaves in</td>
</tr>
<tr>
<td></td>
<td>SmartDashboard.</td>
</tr>
<tr>
<td></td>
<td>• This is also true for Firewall Rules policies that use the same object.</td>
</tr>
<tr>
<td></td>
<td>Changing the object's properties for one policy changes how the object</td>
</tr>
<tr>
<td></td>
<td>behaves in all other Firewall Rules policies.</td>
</tr>
<tr>
<td>(To disable a rule)</td>
<td>After disabling a firewall rule, the rule no longer affects the client.</td>
</tr>
<tr>
<td></td>
<td>You might prefer to disable rules rather than delete and recreate them</td>
</tr>
<tr>
<td></td>
<td>later. Remember that the altered policy must be installed before the</td>
</tr>
<tr>
<td></td>
<td>change takes effect.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deleting a firewall rule automatically removes it from the Security Policy.</td>
</tr>
<tr>
<td></td>
<td>However, the Policy must be reinstalled before the change affects endpoint</td>
</tr>
<tr>
<td></td>
<td>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.
11. To specify the type of tracking, right click the Tracking cell and select Alert, Log, or None.
12. To specify a comment, right click the **Comment** cell, select Edit, and enter text in the window.

To create a Network Object on the Network Objects tab:

1. Click **New**.
2. Select the type of object:
   - Host
   - Address Range
   - Network
   - Site.
3. Click **OK**.
4. In the **Properties** window, enter the needed data: Name, IP address.
5. Click **OK**.

To create a Service on the Services tab:

1. Click **New**.
2. Select the type of service: TCP, UDP, or Group.
3. Click **OK**.
   - In the **Service Properties** window, specify the Name, Port, Color, and Comment. Or:
   - In the **Group Properties** window, add **Available Services** to a group.
4. Click **OK**.

Firewall Rules and Domain Controllers

- **Important** - When creating Firewall Rules for endpoint clients, create explicit rules that allow all endpoints to connect to all of the domain controllers on the network.
Chapter 13

Access Zones Policies

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

There are two Access Zones:

- The Internet Zone
- The Trusted Zone

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

In This Chapter

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Zone</td>
<td>83</td>
</tr>
<tr>
<td>Locations</td>
<td>84</td>
</tr>
<tr>
<td>Creating New Access Zones Definitions</td>
<td>87</td>
</tr>
<tr>
<td>Changing an Existing Access Zones Policy</td>
<td>88</td>
</tr>
</tbody>
</table>

Trusted Zone

The Trusted Zone contains network objects that are trusted. Configure the Trusted Zone to include only those network objects with which your programs must interact.

Note - Objects not placed in the Trusted Zone are placed automatically in the Internet Zone.

The Endpoint Security Management Console contains an initial Access Zones policy. In the initial policy, these network elements are included in the Trusted Zone:

- **All_Internet**
  This object represents all legal IP addresses. In the initial policy, all IP addresses on the Internet are trusted. However, the Access Zones policy is not a policy that is enforced by itself but only as a component of the Application Control and Firewall Rules policies. For example, in the Application Control policy, access permissions are granted for each application or applications group when accessing the Trusted Zone or the Internet Zone. If the initial Access Zones policy is used in an Application Control policy, then the idea of an Internet Zone has no meaning. The Internet Zone is the same as the Trusted Zone.

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

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

Think about adding these objects to your Trusted Zone:

- Remote host computers accessed by your programs (if not included in the subnet definitions for the corporate network)
- Corporate WANs accessed by your programs
- Endpoint Security Management Server
- Domain name servers
- Mail servers
- Domain controllers
- File servers
- Print servers
- VPN gateway address range
- Internet gateways
- Local subnets
- Security servers (for example, RADIUS, ACE, or TACACS servers)
- Other IP addresses or IP ranges to which access is allowed or denied.

Locations

Access Zones are made up of network locations. You define network locations by specifying one or more of the following:

- Host
- IP address range
- Network
- Site

Create network locations for areas that programs must have access to, or areas that programs must be prevented from accessing.

Define locations for each policy or define locations before you create a policy. After defining a location, the location can be reused in other policies.

Note - The Trusted Zone and the Internet Zone can also be used as locations in a firewall policy. These locations are resolved dynamically by the client based on Access Zones policy assignment to the client.

Adding Network Locations

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

To add a network location:

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 location.
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 Location" on page 85)
   - Address Range ("Configuring an Address Range as a Network Location" on page 85)
   - Network ("Configuring a Network as a Network Location" on page 85)
   - Site ("Configuring a Site as a Network Location" on page 86)
   - Group ("Configuring a Group as a Network Location" on page 86)
   - Network Group with Exclusion ("Configuring a Network Group With Exclusion" on page 86)
   - Site Group ("Configuring a Site Group as a Network Location" on page 87)

8. Click OK.

9. Select the location you created, and click the Add button of Trusted Zone Locations. The location is added to the list you selected.

**Configuring a Host as a Network Location**

Enter data that defines the network location:

<table>
<thead>
<tr>
<th>Location Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network location. 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 location.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network location.</td>
</tr>
<tr>
<td>Comment</td>
<td>A description of the network location.</td>
</tr>
</tbody>
</table>

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

Enter data that defines the network location:

<table>
<thead>
<tr>
<th>Location Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network location. 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 location.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color to be used for the icon for this network location.</td>
</tr>
<tr>
<td>Comment</td>
<td>A description of the network location.</td>
</tr>
</tbody>
</table>

**Configuring a Network as a Network Location**

Enter data that defines the network location:

<table>
<thead>
<tr>
<th>Location Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network location. 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 location.</td>
</tr>
</tbody>
</table>
### Configuring a Site as a Network Location

Enter data that defines the network location:

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

### Configuring a Group as a Network Location

1. Enter data that defines the network location:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network location. 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 location.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network location.</td>
</tr>
</tbody>
</table>

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

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

### Configuring a Network Group With Exclusion

Enter data that defines the network location:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the network location. 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 location.</td>
</tr>
</tbody>
</table>
Creating New Access Zones Definitions

Configuring a Site Group as a Network Location

1. Enter data that defines the network location:

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object in</td>
<td>Select a group in which the network location should reside from the drop-down list.</td>
</tr>
<tr>
<td>Except</td>
<td>Select an exception (where the network location should not reside) from the drop-down list.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a description of the network location.</td>
</tr>
</tbody>
</table>

2. Select **New**. The **Site Group Properties** window opens.
3. Select an object from the **Available Objects** column, or create a new object of the type:
   - Site
   - Site Group

Creating New Access Zones Definitions

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

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

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

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

5. Create network locations ("Adding Network Locations" on page 84).
6. Add network locations to **Trusted Zone Locations** by
   - Selecting a network location from the **Available Network Locations**
   - Clicking the **Add** arrow
7. Click **OK**.

*Note* - You cannot reliably use hostnames (such as google, msn etc) 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 locations, and Trusted Zone locations 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 location to the Trusted Zone Locations list:
   - Select a network location from Available Network Locations
   - Click the Add arrow
7. To remove an existing location:
   - Select the network location from the list
   - Click the Remove arrow
8. To delete an existing location, select the location and click Delete.
Chapter 14

Malware Protection Policies

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

The Endpoint Security Management Server regularly receives updated virus and spyware definitions from a Check Point update server. Use policy definitions to check your endpoint computers, enforce regular scans and set treatment options. Either accept the default treatment, client notification and restriction settings, or modify the settings by virus or spyware category.

In This Chapter

Prerequisites 89
Malware Protection - Settings 90

Prerequisites

Before configuring Malware Protection, these steps should be taken.

Configuring a Proxy Server

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

Note - For Anti-malware updates or other program-control related services, you cannot use a proxy that needs NTLM authentication.

To configure a proxy server in Windows:

1. Stop the Check Point Endpoint Security service.
2. Open the following file:
   C:\Program Files\CheckPoint\CPuepm\80.20\engine\conf\local.properties
3. Add the following proxy related 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.
5. Start the Check Point Endpoint Security service.
Enabling Update Traffic
After configuring the proxy server, set up the firewall gateway to accept the traffic to and from the update servers.

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

Port Access
- Endpoint Security server must have access to ports 80 and 443 to retrieve the latest virus and spyware information. Make sure that your firewall gateway allows this traffic.
- If you plan to use Malware Protection in an environment that includes a proxy server for Internet access, configure Endpoint Security server to work with a proxy server.

Malware Protection - Settings
Malware Protection detects and treats viruses (both dormant and active) on the endpoint computer. Files are scanned when opened, run, or closed.

Quick Start

These Malware Protection policies are available:
- Off Malware Protection Policy - Default settings for no malware security.

To assign a policy:
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 from the Navigation tree. Click OK. The assignment is shown on the Assignment window.
5. Click OK.

Creating a Malware Protection Policy
In addition to the predefined policies, you can create a new policy.

To add a new malware protection configuration:
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 and click OK.
Viewing Malware Protection Assignments

You can see all Malware Protection Policies assignments. Single or multiple Policies can be attached to the organization or directories, groups, users, and endpoint computers within the organization.

Multiple policies can be assigned.

To show policy assignments:
1. On the Malware Protection Overview page, click the View By drop-down box
2. Select Assignments.

Malware Protection - Scan Settings

This section describes Anti-virus and Anti-spyware settings that protect endpoint computers against malicious viruses, spyware and riskware.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Level Settings</td>
<td>Select from these scan levels:</td>
</tr>
</tbody>
</table>
|                         | • Custom
|                         | Applies settings configured in the Custom Scan Level Settings window ("Malware Protection Custom Scan Level Settings" on page 92). |
|                         | • Low Scan Level
|                         | Scans:
|                         | • Windows folder, and local startup items only.
|                         | • Local drives and CD |
|                         | • Medium Scan Level
|                         | • Scans local, removable, and CD drives
|                         | • Skips compressed files non-executable files |
|                         | • High Scan Level
|                         | Scans local and removal, and CD drives, and other |
| Scan schedule           | 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 and time. |
| Scan Treatment Settings | Select the Endpoint Security response: |
|                         | • Cure or Delete
|                         | Repairs the file. If repair fails, Endpoint Security deletes the file |
|                         | • Cure or Quarantine
|                         | Attempts to repair the infected file. If the repair fails, Endpoint Security quarantines the file |
## Malware Protection - Settings

### Malware Protection Policies

**Option** | **Description**
--- | ---
Exclude Directories and Processes | Select this option to exclude specific directories and processes from the malware scan. Click **Advanced Settings** ("Malware Protection - Scan Exclusion and Processes" on page 93) to add:
- The fully qualified path to a directory (including its subdirectories) to be excluded from the malware scan.
  Note: all paths must be terminated with a backslash, for example: `driveletter:\folder\`
- The fully qualified path to a trusted executable to be excluded from the malware scan.

Signature and Engine Update Settings | Configure the frequency, in hours, between client requests for malware signature and scanning engine updates.

---

### Malware Protection Custom Scan Level Settings

Customized Malware Protection scan level settings give 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, showing:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan File Types</strong></td>
<td>Select one of these options:</td>
</tr>
<tr>
<td>- Quick Scan</td>
<td>Scans the <strong>Windows</strong> folder, subfolders and startup items as defined by Kaspersky.</td>
</tr>
<tr>
<td>- Normal Scan</td>
<td>Scans all files except compressed files and non-executable files.</td>
</tr>
<tr>
<td>- Deep Scan</td>
<td>Scans all file types.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Scan Targets</strong></th>
<th>Select from these scan targets:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <strong>Removable</strong>:</td>
<td>Scans removable media devices, such as USB.</td>
</tr>
<tr>
<td>- <strong>CD-ROM</strong>:</td>
<td>Scans CD-ROMs.</td>
</tr>
<tr>
<td>- <strong>Other</strong>:</td>
<td>Any device which Windows recognizes as a drive.</td>
</tr>
</tbody>
</table>

**Note:** By default, the local drive is always selected.

**Do not scan files larger than...** | Do not include files above a certain size if scanning them significantly reduces computer performance.

**Optimize scan by storing file checksums** | Optimize the scan by storing file checksums on the server during the first scan. During subsequent scans, only new files or files whose checksum has changed are scanned.

**Optimize scan by storing NTFS file system data** | NTFS cluster size, file name, folder structure are stored on the server during the first scan. Only places where the file size, name, or structure has changed are included in subsequent scans.

**Note** - Customized scans significantly impact endpoint performance. Run customized scans during times when users are not logged into their computers.
Malware Protection - Scan Exclusion and Processes

You can exclude the contents of trusted directories and specified trusted program executables from the Malware Protection scan. These are suggested factors for excluding a directory or program 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 process lets the specified, trusted executable run. Excluding a folder prevents the Anti-malware scanner from examining the folder contents.

To exclude a directory from a scan:
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 Processes option. This option must be selected to enable directory exclusion.
4. Click Advanced Settings or select Scan Exclusion and Processes from the tree.
5. In the Scan Exclusion and Processes pane, 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 the directory path.
   Example: C:\Program Files\MyTrustedDirectory\  
7. Click OK.
   The trusted directory shows in the Scan exclusions list.

To exclude a trusted program executable 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 Processes option. This option must be selected to enable program exclusion.
4. Click Advanced Settings or select Scan Exclusion and 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 to the trusted executable file.
   Example: C:\Program Files\MyTrustedDirectory\MyTrustedProgram.exe
7. Click OK.
   The trusted program shows in the Trusted Processes list.

Malware Protection - Assignment Settings

To assign a policy:
1. On the Compliance Rules Policy Overview page, open an existing policy or create a new one.
3. Click Assignment in the navigation tree.
4. Click Add Assignment.
5. Click Connected to enterprise.
   The Select Node window opens.
6. In the Navigation Tree, select a node in the directory. When selecting a directory or group, users belonging to that group or directory show in the Node area.
7. Click OK.
8. On the Assignment page, click the Add Assignment down arrow, and select from the displayed options.
9. Click OK.
10. Click Save & Install.
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 Save & Install.
Chapter 15

Application Control Policies

Application Control restricts network access of applications that act as either clients or servers.

To access Application Control settings:

Open Policies tab > Application Control.

In the Policies > Application Control window, you see the configurations that are currently available to you. An Application Control configuration includes a set of access permissions for programs.

When you have created an Application Control configuration, you can add it to a policy in the Policies > Overview window. Users and computers in your Active Directory get the policy and then the Endpoint Security clients enforce the permissions.

In This Chapter

Creating Application Control Configuration 95
Understanding Application Groups 96
Permissions 96
How Application Control Functions 98
Planning Application Control 99
Monitoring Applications - Automatic Add 102
Creating Custom Program Groups 102
Changing Group Definitions 103
Deleting Program Groups 103
Managing Unknown Applications 103
Program Permissions and Disconnected Policies 104
Importing Programs 104
Manually Adding Programs 107
Program Advisor 107

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:

- **PA terminated applications**: Applications that Program Advisor recommends terminating because they are known to be malicious.
- **Critical Services**: Applications that must have these permissions, or the endpoint will not function correctly. For example: LSASS and svchost.
- **Secondary Services**: Services and applications that should have these permissions for correct functioning.
- **PA referenced Applications**: Applications that Program Advisor recommends allowing.
- **Unknown Applications**: 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).

<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.</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</td>
</tr>
<tr>
<td></td>
<td>sure that applications are moved out this group (filters are created for other groups that will pull in</td>
</tr>
<tr>
<td></td>
<td>matching applications from this group).</td>
</tr>
</tbody>
</table>

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

**Custom Groups**

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

Some possible uses for custom groups include:

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

**Permissions**

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

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

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

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

Therefore, the possible permissions for a program are:

*Table 15-2 Permission Options*

<table>
<thead>
<tr>
<th>Zone + Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted + Client</td>
<td>Permission of program on endpoint computer to connect to a server that is in the defined Trusted Zone.</td>
</tr>
<tr>
<td></td>
<td>For example, Outlook permissions to connect to an Exchange server.</td>
</tr>
<tr>
<td></td>
<td><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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><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 as little as possible. This setting enlarges the policies, both Connected and Disconnected, and may adversely affect performance.

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

Program Permission Lifecycle Use Case

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

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

The recommended flow is:

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

Unknown Program Configuration - Use Case

This example shows how to implement the recommendation to start with less disruptive (more lenient) permissions for Unknown Programs, and gradually monitor and change to more secure.
Each phase in the use case is evaluated for the following criteria:

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

### Table 15-3 Unknown Program Permissions - Use Case

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

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

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

### Phase 1: Block Internet Zone Servers Only

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

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

#### Table 15-4 Impact of Blocking Internet Zone Server Role

<table>
<thead>
<tr>
<th>Impact area</th>
<th>Level</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown attack protection</td>
<td>Good</td>
<td>Any unknown application that tries to accept a connection from the Internet Zone is blocked.</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.
### Table 15-5 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.

### Table 15-6 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.

### Table 15-7 Impact of White Listing

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

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

To monitor controlled applications:
2. Right-click an application group and select Edit Applications.

The Applications window opens.

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

Creating Custom Program Groups

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

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

To create a custom program group:
1. Open Policies > Application Control > Program Groups.
2. Right-click in the Program Groups table where you want to add the new group, and select Add Group.
3. Click either Above or Below, to add the new group to the list in relation to the selected group.

   The Add Program Group window opens.
4. Provide a name and optional comment for the group.
5. If this group should maintain the permissions set here even when clients are disconnected from the Endpoint Security system, select Enable this group in disconnected policies. However, note that this setting is not recommended (to ensure performance).
6. Set the group permissions.
7. In the Program Filter list, click Add.

   The Program Filter window opens.

8. Provide the criteria that determine which programs are added to this group automatically when they are observed running on an endpoint.
### 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 Windows 95, 98, or ME operating systems, you also need to copy `unicows.dll`, located in the `<installdir>checkpoint\Integrity\engine\webapps\ROOT\bin` directory on the Endpoint Security host, to the root directory (typically `c:\`) of the baseline reference source computer.

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

2. On the protected computer, in the command prompt, go to the root directory or to a specific directory to scan (for example, `\program files`).

3. Type `appscan` to begin the scan.

   You can modify the scan through the use of the Appscan switches.

   When the scan is complete, an output file (`scan.xml`) is created in the directory where you ran the scan.

   Your Appscan file is ready to be imported into Endpoint Security.

**Appscan Switches**

Use the following switches to modify your scan.

*Table 15-9 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>Example 1: <code>C:\appscan /o scan1.xml [files]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>If you conduct multiple scans on the same machine, give each scan a unique name.</td>
</tr>
<tr>
<td><code>/x</code></td>
<td>Designates target file names to add to the scan.</td>
</tr>
<tr>
<td></td>
<td>- The leading period before a file extension is required.</td>
</tr>
<tr>
<td></td>
<td>- A semi-colon separates the target extensions.</td>
</tr>
<tr>
<td></td>
<td>- The target extensions are grouped by quotes.</td>
</tr>
<tr>
<td></td>
<td>- A target directory must be specified using the <code>/s</code> switch.</td>
</tr>
<tr>
<td></td>
<td>- If the <code>/x</code> switch is not used in the command statement: Only program files (.exe file name extension) are scanned.</td>
</tr>
<tr>
<td>Example 2: <code>C:\appscan /o scan2.xml /x &quot;.exe;.dll&quot; /s &quot;C:\&quot;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Example 2, the scan is named <code>scan2</code>, and the scan will include .exe and .dll files in the current directory only.</td>
</tr>
</tbody>
</table>
### Switches and Functions

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s</td>
<td>Designates the directory for SmartSum to inventory.</td>
</tr>
<tr>
<td></td>
<td>• If you do not use /s to designate a target directory, the scan will be run in the current directory only.</td>
</tr>
<tr>
<td></td>
<td>• If you use /s, the scan will be run in the target directory and its subdirectories.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 3</strong>: C:\appscan /o scan3.xml /x &quot;.dll&quot; /s c:\program files</td>
</tr>
<tr>
<td></td>
<td>In Example 3, the scan is named <code>scan3</code>. The target directory is <code>C:\program files</code> and all its subdirectories. The target extension is <code>.dll</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 4</strong>: C:\appscan /o scan4.xml /x &quot;.exe;.dll&quot; /s c:\program files</td>
</tr>
<tr>
<td></td>
<td>In Example 4, the scan is named <code>scan4</code>. The target directory is <code>C:\program files</code>. The target extensions are <code>.exe</code> and <code>.dll</code>.</td>
</tr>
<tr>
<td>/e</td>
<td>Use the <code>/e</code> switch to inventory all executable files in the target directory or drive, regardless of extension.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 5</strong>: C:\appscan /s &quot;C:\program files&quot; /e</td>
</tr>
<tr>
<td></td>
<td>In Example 5, all files are incorporated into the scan.</td>
</tr>
<tr>
<td>/a</td>
<td>Generates all file properties for each file inventoried.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 6</strong>: C:\appscan /o scan6.xml /s &quot;C:&quot; /a</td>
</tr>
<tr>
<td></td>
<td>In Example 6, the scan is named <code>scan6</code>. The target directory is the entire contents of <code>C:\</code>. The output file displays file properties more thoroughly than it would without the <code>/a</code> switch. The <code>/a</code> switch does not affect the source.</td>
</tr>
<tr>
<td>/p</td>
<td>Displays progress messages.</td>
</tr>
<tr>
<td>/verbose</td>
<td>Displays progress and error messages.</td>
</tr>
<tr>
<td>/warnings</td>
<td>Displays warning messages.</td>
</tr>
<tr>
<td>/? or /help</td>
<td>Displays help for Appscan.</td>
</tr>
</tbody>
</table>

### 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:
1. In C:\Program Files\CheckPoint\CPuepm\R70\engine\conf, open the local.properties file.
2. Add the following properties, and then stop and restart the Endpoint Security Management Server.

```
http.proxyHost=host-name-or-ip
http.proxyPort=proxy-port
http.proxyUser=username
http.proxyPassword=password
```
Chapter 16

Endpoint Compliance

Endpoint Compliance makes sure that:

- Endpoint Security packages, operating system service packs, and updates are installed on an endpoint computer.
- Only permitted programs are installed on the endpoint.

More restrictive firewall, Access Zones, Application Control, and Media Encryption & Port Protection policies might be applied to an endpoint that fails to match the requirements of the compliance policy.

Logs showing endpoint compliance and remediation are available through SmartView Tracker.

In This Chapter

Compliance Status 109
Quick Start 110
Planning Compliance Rules 110
Creating a Endpoint Compliance Policy 110
Viewing Endpoint Compliance Policy Assignments 111
Endpoint Compliance Policy 111
Endpoint Compliance Assignment 113
Check Object 113

Compliance Status

The Compliance Status area on the Overview tab shows the percentage of endpoint computers for each compliance category.

To show compliance status by organization:
1. From the Monitor area on the Overview tab, select the Compliance Status report.
2. Click the My Organization browse button to select the scope of the report.
   - The report can cover all the organization, a directory, network, group, user, or one endpoint computer.
   - The pie chart shows the percentage of endpoint computers that match the predefined compliance categories.

To show compliance status by user:
1. Click Show Details.
2. From Filter, select User Name or Machine Name.
3. From Statuses, select All or one of the status categories.
4. The compliance status of individual users is shown in the table.

Note - Click Export to File to copy the compliance status information shown in the table to Excel or CSV.
Quick Start
This section explains how to quickly assign predefined Endpoint Compliance policies.

These Endpoint Compliance policies are available:

- **High Security Compliance Level** - Recommended consistent endpoint security, functionality and maintenance in a large environment.
- **Medium Security Compliance Level** - Recommended for consistent endpoint security and maintenance. Users can install and use worked-related applications.
- **Low Security Compliance Level** - Recommended for control of endpoint security, without required operating system update level or application control.

To assign a policy:
1. On the Endpoint Security Management Server console, click the **Policies** tab and select **Endpoint Compliance Policies** on the **Navigation** tree.
   The **Endpoint Compliance Overview** page opens.
2. Double-click one of the predefined policies.
   The **Endpoint Compliance Policy** window opens.
3. Click **Assignment**.
   On the **Assignment** window, click **Add Assignment** and select from the **Navigation** tree. Click **OK**.
   The assignment is shown on the **Assignment** ("Endpoint Compliance Assignment" on page 113) 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 Endpoint Compliance Policy
This section explains how to create an Endpoint Compliance policy.

To create a compliance rules policy:
1. In the Endpoint Security Management Console, open the **Policies** tab.

3. From View By, select Policies.

4. Click New.

5. The Endpoint Compliance Policy window opens.

6. Configure the compliance settings.

7. Click OK.

8. Click Save & Install.

Viewing Endpoint Compliance Policy Assignments

Policies can be assigned to all of the organization, networks, directories, groups, and users. Multiple policies can be assigned to the user and endpoint computer.

To show policy assignments:
1. On the Policy tab > click Compliance Rules in the navigation tree.
2. From the View By drop-down box, Select Assignments.

Endpoint Compliance Policy

This section explains how to configure Endpoint Compliance for Endpoint Security packages, operating system service packs, and application control.

Before configuring a compliance policy:
1. Open the Endpoint Security Management Console
2. Open Manage > General Properties and configure these settings:
   - Connection Settings ("Configuring the Heartbeat Interval" on page 50)
     Make sure to set:
     - An interval between heartbeats
     - For how many heartbeats the endpoint can be out of compliance (5 by default)
   - Authentication Settings ("Understanding Endpoint Security Authentication" on page 39)

General Configuration

To Configure a Compliance Policy:
1. In the Endpoint Security Management Console, open the Policies tab.
2. On the navigation tree, click Compliance Rules.
3. From the View By drop-down box, select Policies.
4. Double-click an existing policy or create a new one.
   The Compliance Rules Policy window opens.
5. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security Client</td>
<td>Monitors the client's version. Click Manage to add or remove a Deployment Profile Check object. The Client Profile Check object makes sure that the Endpoint Security package specified in the profile is installed on the user's computer.</td>
</tr>
</tbody>
</table>
## Endpoint Compliance Policy

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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  
  - File name and its properties |
| **Required Applications & Files** | Checks for required applications. Click **Manage** to add or remove an Application Check object. An Application Check object is used to identify:  
  - An application registry key and value  
  - File name and its properties |
| **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 |
| **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.

### Custom Rules

Custom rules can also be used to configure an Endpoint Compliance policy. Compliance values selected in **General Properties** for Endpoint Security packs, operating system service packs, and application controls are displayed here.

**Custom Rules** let you identify rules by a unique rule name. Use the **Custom Rule** buttons to set the sequence in which messages show on the endpoint after a compliance violation.
Endpoint Compliance Assignment

For compliance to work, Endpoint Compliance policy must be assigned to:

- A user
- An endpoint computer or group of endpoint computers.

If assigned to a computer, all users of that computer receive the same policy. If assigned to a user, the policy is unique to that user.

**To assign a policy:**
1. On the **Compliance Rules Policy Overview** page, open an existing policy or create a new one.
2. The **Compliance Rules Policy** window opens.
3. Click **Assignment** in the navigation tree.
4. Click **Add Assignment**.
5. Click **Connected to enterprise**.
   The **Select Node** window opens.
6. In the **Navigation Tree**, select a node in the directory. When selecting a directory or group, users belonging to that group or directory show in the **Node** area.
7. Click **OK**.
8. On the **Assignment** page, click the **Add Assignment** down arrow, and select from the displayed options.
9. Click **OK**.
10. Click **Save & Install**.

**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 **Save & Install**.

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><strong>Check Registry</strong></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><strong>Registry Key</strong></td>
<td>Enter the registry key to identify.</td>
</tr>
<tr>
<td><strong>Registry Value</strong></td>
<td>Enter the registry value that matches the Check Registry type.</td>
</tr>
<tr>
<td><strong>Check File</strong></td>
<td>Select one of these to check if an application is running or if a file exists:</td>
</tr>
<tr>
<td></td>
<td>- <strong>File is running at all times</strong> - For example, make sure that Endpoint Security client is always running.</td>
</tr>
<tr>
<td></td>
<td>- <strong>File exists</strong> - For example, make sure that the user browsing history is always kept.</td>
</tr>
<tr>
<td></td>
<td>- <strong>File is not running</strong> - For example, make sure that DivX is not used.</td>
</tr>
<tr>
<td></td>
<td>- <strong>File does not exist</strong> - For example, make sure that a faulty dll file is removed.</td>
</tr>
<tr>
<td><strong>File Name</strong></td>
<td>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)</td>
</tr>
<tr>
<td><strong>File Path</strong></td>
<td>Enter the path, but do not include the file name.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Use environment Variables of logged in user</strong> attribute includes paths defined in the endpoint computer's system and user variables.</td>
</tr>
<tr>
<td><strong>Check File Properties</strong></td>
<td>Additional options to check for an existing or non-existing file.</td>
</tr>
<tr>
<td><strong>Match File Version</strong></td>
<td>Make sure that a specific version or range of versions of the file or application complies with the file check.</td>
</tr>
<tr>
<td><strong>Match MD5 Checksum</strong></td>
<td>Find the file by MD5 Checksum. Click <strong>Calculate</strong> to compare the checksum on the endpoint with the checksum on the server.</td>
</tr>
<tr>
<td><strong>File is not older than</strong></td>
<td>Find the file by the number of days on the endpoint computer.</td>
</tr>
</tbody>
</table>
Remediation Objects and Client Remediation Messages

A Remediation object runs an application or file to make the endpoint computer compliant. To see the list of Remediation objects, open Custom Rules > Remediations tab.

To create a Remediation object:
   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>Operations</td>
<td></td>
</tr>
<tr>
<td>Run Custom File</td>
<td>Activates the Run Custom File option.</td>
</tr>
<tr>
<td>Download Path</td>
<td></td>
</tr>
<tr>
<td>• The Download Path is a temporary directory on the local machine 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).</td>
<td></td>
</tr>
<tr>
<td>• The path cannot be empty.</td>
<td></td>
</tr>
<tr>
<td>• The endpoint client first tries to access the file from the specified path. If the client fails, it downloads the file from the URL to the temporary directory and runs it from there.</td>
<td></td>
</tr>
<tr>
<td>• To run multiple files, use one of the popular compression programs such as WinRar to produce a self-extracting executable that contains a number of .exe or .bat files.</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>• Enter the URL of an http file share server where the file is located.</td>
<td></td>
</tr>
<tr>
<td>• Enter the full path that includes the actual file with one of the supported extensions (*.bat or *.exe).</td>
<td></td>
</tr>
<tr>
<td>• This path can be left empty.</td>
<td></td>
</tr>
<tr>
<td>• Make sure the file share is not protected by a username or password.</td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>If the executable specified in the URL runs an installation process, make sure that the executable holds a parameter that specifies the directory where the program should be installed. If the executable does not hold such a parameter, enter one here.</td>
<td></td>
</tr>
<tr>
<td>MD5 Checksum</td>
<td>Click Calculate to generate a MD5 Checksum, a compact digital fingerprint for the installed application.</td>
</tr>
<tr>
<td>Run as System</td>
<td>Apply system rights for running the executable file. Not all processes can run with user rights. System rights may be required to repair registry problems and uninstall certain programs.</td>
</tr>
<tr>
<td>Run as User</td>
<td>Apply user rights and local environment variables for running the executable file.</td>
</tr>
<tr>
<td>Messages</td>
<td></td>
</tr>
<tr>
<td>Automatically execute operation without user notification</td>
<td>Run the executable file without displaying a message on the endpoint computer.</td>
</tr>
<tr>
<td>Execute operation only after user notification</td>
<td>Run the executable file only after asking approval.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</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. A Non-Compliant message tells the user that the endpoint computer is non-compliant and provides details of how to achieve compliancy. A Restricted message tells the user that the endpoint computer is non-compliant, provides details of how to achieve compliancy, and restricts computer use until compliancy is achieved.</td>
</tr>
<tr>
<td>Message Box</td>
<td>Displays selected non-compliant and restricted messages. The message box is available only by selecting the Execute only after user notification setting. Click Add, Remove, or Edit to add a message, and remove or revise a selected message. Note: The user cannot prevent the remediation application or file from running.</td>
</tr>
</tbody>
</table>

**Client Message Properties**

When Warning or Restricted is the selected action on a compliance check, such as Prohibited Applications & Files, a message shows on the client.

**To create a client text message:**

1. Open the Compliance Rule Policy > General Properties page.
2. For a specified compliance check, click Manage.
   The Run File Remediation Properties window opens.
3. In the Messages area, click Add.
   The New Client Message Properties window.
4. From the Locale drop down box, select a language for the message.
5. From the Non-compliant Message or Restrict Message drop-down box:
   - Select an existing message or
   - Click Manage to create a new one.
   The Client Messages Properties window opens.
6. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Select the language.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the message title.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the message text.</td>
</tr>
<tr>
<td>Confirmation Text</td>
<td>The text displayed in the message for the user to click as confirmation.</td>
</tr>
</tbody>
</table>
7. Click OK.
   The new client message shows in the Remediation Message box.

**Group Check Properties**

A Group Check object is a container that holds multiple check objects (application checks, service pack checks, custom checks).

**To create a Group Check object:**

1. On the Policies tab > Compliance Rules page, open an existing policy (or create a new one).
   The Compliance Rules Policy window opens.
   The Select New Object Type window opens.
3. From the list, select Group Check.
   The Group Check Properties window opens.
4. Configure the endpoint to satisfy all the checks in the list, or only one of them.
5. Click **Add > New** to create more check objects.

**Client Profile Check Properties**

The Client Profile Check object identifies Endpoint Security endpoint computers for update purposes.

**To create a client profile check:**

1. On the **Policies** tab > **Compliance Rules** page, open an existing policy (or create a new one).
   
   The **Compliance Rules Policy** window opens.
2. On the **Custom Rules** page > **Checks** tab, click **New**.
   
   The **Select New Object Type** window opens.
3. From the list, select **Client Profile Check**.
4. The **Client Profile Check Properties** Window opens.
5. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Select the deployment profile. The profile identifies the endpoint package version.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the Windows version.</td>
</tr>
</tbody>
</table>

**Service Pack Check Properties**

A Service Pack Check object identifies Window operating system files on the endpoint computer that must be updated.

**To create a Service Pack check:**

1. On the **Policies** tab > **Compliance Rules** page, open an existing policy (or create a new one).
   
   The **Compliance Rules Policy** window opens.
2. On the **Custom Rules** page > **Checks** tab, click **New**.
   
   The **Select New Object Type** window opens.
3. From the list, select **Service Pack Check**.
4. The **Service Pack Check Properties** Window opens.
5. Configure these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Select the Windows version</td>
</tr>
<tr>
<td>Registry Key</td>
<td>Enter the registry key for the service pack.</td>
</tr>
<tr>
<td>Registry Value</td>
<td>Enter the registry value for the service pack.</td>
</tr>
</tbody>
</table>
Chapter 17

WebCheck

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.

WebCheck supports these browsers:
- Internet Explorer, versions 6, 7, 8
- Mozilla Firefox, versions 2, 3

In This Chapter

<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 119) that are safe to exclude from WebCheck.</td>
</tr>
</tbody>
</table>

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.

Creating Trusted Sites

Temporarily Disabling WebCheck
Creating Trusted Sites

A trusted site is a site for which WebCheck is not required. For example a site within the corporate network would be considered safe and therefore trusted. With the trusted sites option, WebCheck creates different browsing environments:

- One for trusted sites within the corporate zone.
- One for the non-trusted Internet zone.

Trusted sites are opened directly in the end-user’s browser. Non-trusted sites are opened in the WebCheck virtual browser.

To Create a Trusted Site or Group of Sites:
1. Open the Endpoint Security Management Console.
2. On the Policies tab, select WebCheck.
   The WebCheck Policy window opens.
   This adds WebCheck to the policy.
5. Click WebCheck trusted sites.
6. Click Add, and select Site Pattern Properties.
7. In the Site Pattern Properties window, enter:
   a) A descriptive name in the Name field.
   b) A Host Name according to one of the permitted formats:

<table>
<thead>
<tr>
<th>Permitted Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>company.com</td>
<td>Domain name for a single host</td>
</tr>
<tr>
<td><a href="http://www.company.com">www.company.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.*.company.com">www.*.company.com</a></td>
<td>Domain with wild card for sub-domain</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>IP address for a single host</td>
</tr>
</tbody>
</table>

   Note - URLs are not permitted.
8. Click Add > New > Site Pattern Group to collect single sites into an easily managed group.

Temporarily Disabling WebCheck

In rare cases, WebCheck can interfere with normal browsing. To resolve these issues, Check Point supplies a utility (NOISW.exe), that lets users temporarily disable WebCheck protection. This utility is not documented in the Endpoint Security User Guide. We recommend that you do not tell users about NOISW.exe, unless there are no alternatives that resolve the issue.

When a user runs NOISW.exe, WebCheck is disabled for a user-defined period of time. An alert appears in the WebCheck Status pane on the Monitoring tab.

To let a user temporarily disable WebCheck, give these instructions:
1. Close all Web browsers.
2. Run NOISW.exe, located in the Program Files\CheckPoint\Endpoint Security\WebCheck folder.
3. Enter the number of minutes to disable WebCheck. The default is 15 minutes.
4. In the WebCheck window, click Suspend.
5. Click OK to confirm.
Chapter 18

Common Client Settings

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

A Common Client Settings policy is a policy shared by a number of endpoints, these endpoints being Organizational Units in the Active directory, corporate groups (such as HR, Finance) specific users or single computers. A common policy is created in the Common Client Settings Overview window.

In This Chapter

Common Client Window 120
Setting a Common Client Policy 120

Common Client Window

The Common Client Settings Policy Overview window lets you:

- View how current policies are assigned
- Create new policies
- Edit current policies
- Add or remove policies

A Common Client Settings policy can be set for:

- User interface settings
- The client uninstall password
- Uploading log files to the server
- 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 page opens.
4. On the General Properties page, configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for the policy</td>
</tr>
<tr>
<td>Notification Area Settings</td>
<td>Decide whether the client icon should display in the windows notification area and if so, whether the right-click menu is available.</td>
</tr>
</tbody>
</table>
## Setting a Common Client Policy

### Common Client Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Install / Uninstall Settings</strong></td>
<td>- <strong>Enable silent restart upon client upgrade.</strong> Select this option to reboot the endpoint computer after a client installation.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Client Uninstall Password.</strong> A password that the end user must enter before uninstalling the client.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Legacy Client Uninstall Password.</strong> A password that the end user must enter before uninstalling a legacy client</td>
</tr>
<tr>
<td><strong>Log Upload Settings</strong></td>
<td>Conditions that must be met before logs are uploaded to the server. The following blades upload logs to the Endpoint Security Management Server:</td>
</tr>
<tr>
<td></td>
<td>- Desktop Firewall</td>
</tr>
<tr>
<td></td>
<td>- Application Control</td>
</tr>
<tr>
<td></td>
<td>- Anti-malware, compliance)</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>- WebCheck</td>
</tr>
<tr>
<td><strong>Network Protection Settings</strong></td>
<td>- <strong>Allow network protection shutdown</strong></td>
</tr>
<tr>
<td></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>
</tr>
<tr>
<td></td>
<td>- Alerts are client-side pop-up messages. This setting determines whether alerts should be switched on and logged.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
6. In the navigation tree, select **Assignment**.
7. The **Assignment** page shows.
8. 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.
9. In the **Select Node** window, select a node from the Active Directory. Each node represents an object in the organizational tree.
   **Note** - An existing assignment can be removed, or a different policy assigned.
10. Click **OK**. A Common Client policy has been created and assigned.
11. On the **File** menu, click **Save**.
Chapter 19

Remote Help

Users can be denied access to their Full Disk Encryption-protected endpoint computers or Media Encryption & Port Protection-protected devices for a number of reasons. For example, they might have entered an incorrect password too many times or forgotten their password or, in a worst case scenario, a hacker might have tried to break into their computer or device.

Remote Help is designed to assist users in these types of situations. The user calls the designated Endpoint Security administrator and follows the Remote Help procedure.

Note - An Endpoint Security administrator can provide Remote Help to users who have been denied access to their Full Disk Encryption protected computers, or computers with Media Encryption & Port Protection only if you enabled Remote Help in the OneCheck User Settings policy.

In This Chapter

Remote Help Types 122
Process for Remote Help 122
Providing Full Disk Encryption Remote Help 123
Providing Media Encryption & Port Protection Remote Help 123
Disabling Remote Help 124

Remote Help Types

There are two types of Full Disk Encryption Remote Help:

- **One Time Login** - One Time Login allows access as an assumed identity for one session, without resetting the password. If users lose their Smart Cards, they must use this option.

- **Remote password change** - This option is for users who use fixed passwords and have forgotten them. For devices protected by Media Encryption & Port Protection policies, only remote password change is available.

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 • 47
Access to Media Encryption & Port Protection Policies • 74
Access Zones Policies • 83
Account Lockout • 56
Activity Reports • 29
Adding Network Locations • 84
Advanced Media Log • 77
Anti-Malware • 30
Application Control Policies • 95
Appscan Switches • 105
Assigning Policies • 50

B

Backup and Restore • 23

C

Centralized Deployment • 12
Centralized Monitoring • 12
Centralized Organization of Users and Computers • 11
Changing a User's Logon Preboot Password • 27
Changing an Existing Access Zones Policy • 88
Changing Group Definitions • 103
Changing the Clean Up Task Status • 16
Changing the Group Ranking Order • 78
Check Object • 113
Client logging • 33
Client Packages • 35
Client Profile Check Properties • 117
Client Requirements for Full Disk Encryption Deployment • 68
Common Client Settings • 120
Common Client Window • 120
Compliance Status • 29, 109
Configuring a Client Package with a Default VPN Site • 37
Configuring a Group as a Network Location • 86
Configuring a Host as a Network Location • 85
Configuring a Network as a Network Location • 85
Configuring a Network Group With Exclusion • 86
Configuring a Site as a Network Location • 86
Configuring a Site Group as a Network Location • 87
Configuring Active Directory for Authentication • 42
Configuring an Address Range as a Network Location • 85
Configuring and Installing Initial Package • 41
Configuring Authentication • 40
Configuring Authentication Settings • 43
Configuring Client Packages • 36
Configuring Connected, Disconnected or Restricted State • 49
Configuring the Apache Cache • 15
Configuring the Directory Scanner • 20
Configuring the Heartbeat Interval • 50
Configuring VPN Client Settings • 38
Connected, Disconnected or Restricted • 48
Creating a Customized Full Disk Encryption Policy • 61
Creating a Endpoint Compliance Policy • 110
Creating a Malware Protection Policy • 90
Creating an Appscan • 105
Creating Application Control Configuration • 95
Creating Custom Access Rules for Data • 76
Creating Custom Media Authorization Settings • 77
Creating Custom Program Groups • 102
Creating Exceptions to Device Logging • 78
Creating Firewall Rules • 82
Creating New Access Zones Definitions • 87
Creating Trusted Sites • 119
Custom Check and Application Compliance Check Properties • 114
Custom Rules • 112

D

Deleting Program Groups • 103
Demo and Product Licenses • 17
Deploying Policies • 53
Deploying Subsequent Client Packages • 44
Deployment Mode Process • 68
Direct Assignment • 50
Directory Scanner • 19
Directory Synchronization • 21
Disabling Remote Help • 124
Drive Encryption • 61
Dynamic Mount Utility • 73

E

Editing Program Group Permissions • 98
Editing Specific Program Permissions • 98
Enabling WebCheck • 118
Encrypting Removable Media • 76
Endpoint Agent Installations and Upgrades • 33
Endpoint Compliance • 109
Endpoint Compliance Assignment • 113
Endpoint Compliance Policy • 111
Endpoint Security License Types • 17
Endpoint Security Licenses • 17
Endpoint Security Licensing • 59
Endpoint Security Services and Ports • 10
Evaluation Mode Client • 41
Evaluation Mode License • 59
Example 1 • 81
Example 2 • 81
Examples of Rule Numbers • 81
Exporting Packages • 41
Finding Components in the Console • 31
Firewall Rule Number • 81
Firewall Rules - Control Icons and Buttons • 79
Firewall Rules Policies • 79
Firewall Rules Policy Options • 79
Full Disk Encryption • 30, 60
Full Disk Encryption Deployment Mode • 72
Full Disk Encryption Installation and Deployment • 68

F

Finding Components in the Console • 31
Firewall Rule Number • 81
Firewall Rules - Control Icons and Buttons • 79
Firewall Rules Policies • 79
Firewall Rules Policy Options • 79
Full Disk Encryption • 30, 60
Full Disk Encryption Deployment Mode • 72
Full Disk Encryption Installation and Deployment • 68
Full Disk Encryption Licenses • 70
Full Disk Encryption Logs • 72
Full Disk Encryption Recovery • 69
Full Disk Encryption Troubleshooting • 70

G
General Configuration • 111
General Properties • 75
Getting and Applying Contracts • 18
Getting Licenses • 18
Global Package Configurations • 37
Global Settings on the Overview Page • 74
Group Assignment Priority • 51
Group Check Properties • 116

H
Handling Client Packages • 44
How Application Control Functions • 98
How to Back Up and Restore • 23

I
Important Information • 3
Importing Appscans • 106
Importing Programs • 104
Inherited Assignment • 51
Installing and Deploying Endpoint Security Clients • 32
Installing Endpoint Security Management Console • 16
Installing Endpoint Security Management Server • 13
Installing External Endpoint Policy Servers • 16
Installing the Client Using the CLI • 33
Installing the Client Using the EPS.msi File • 32
Installing the Server • 14
Introduction • 8

L
License Behavior • 18
License Status • 19
Locations • 84

M
Malware Protection - Assignment Settings • 93
Malware Protection - Scan Exclusion and Processes • 93
Malware Protection - Scan Settings • 91
Malware Protection - Settings • 90
Malware Protection Custom Scan Level Settings • 92
Malware Protection Policies • 89
Managing Networks • 27
Managing Policies and Users • 47
Managing Unknown Applications • 103
Manually Adding Programs • 107
Media Encryption & Port Protection • 30
Media Encryption & Port Protection Policies • 74
Media Encryption & Port Protection Terminology • 74
Minimal Deployment Mode Configuration • 68
Monitoring Applications - Automatic Add • 102
Monitoring Tab • 28
My Organization Tab • 26

N
Non-Compliance • 48

O
Offline Upgrades • 46
OneCheck Logon • 67
OneCheck Logon Assignments • 55
OneCheck Settings Policies • 54
Online Upgrades • 46
Organization-Centric model • 11
Overriding Preboot Settings • 66
Overview of the System Architecture • 9
Overview tab • 26

P
Password Security • 56
Password Security - Custom Level • 56
Permission Precedence • 97
Permissions • 57, 96
Phase 1
  Block Internet Zone Servers Only • 100
Phase 2
  Block All Servers • 100
Phase 3
  Block All Non-trusted Communication • 101
Phase 4
  White Listing • 101
Planning Application Control • 99
Planning Compliance Rules • 110
Planning Endpoint Security Management Server Installation • 13
Plug and Play License • 59
Policies Tab • 28
Policy Assignment • 67
Policy Assignment Order • 51
Policy-centric Model • 12
Preboot Protection • 62
Prerequisites • 23, 89
Prerequisites for Installation • 14
Primary Full Disk Encryption Components • 69
Process for Remote Help • 122
Product License • 59
Program Advisor • 107
Program Advisor Server • 107
Program Permission Lifecycle Use Case • 99
Program Permissions and Disconnected Policies • 104
Properties for OneCheck User Settings • 55
Providing Full Disk Encryption Remote Help • 123
Providing Media Encryption & Port Protection Remote Help • 123
Providing Software Signatures • 38

Q
Quick Start • 54, 60, 90, 110

R
Recommendations for Management • 52
Remediation Objects and Client Remediation Messages • 115
Remote Help • 65, 122
Remote Help Types • 122
Role-Based Administration • 58
S
Scanning Computers • 104
Scheduling a New Clean up • 16
Service Pack Check Properties • 117
Setting a Common Client Policy • 120
Setting Device Categories to Log • 78
Setting Directory Scanner Credentials • 19
Software Blades • 11
Software Deployment • 29
Software Deployment Tab • 31
State of Compliance • 48

T
Temporarily Disabling WebCheck • 119
Troubleshooting Authentication • 40
Troubleshooting the Directory Scanner Configuration • 21
Troubleshooting the Installation • 34
Trusted Zone • 83

U
Understanding Application Groups • 96
Understanding Endpoint Security Authentication • 39
Uninstalling the Client • 35
Unknown Program Configuration - Use Case • 99
Updating the PAT Version on the Server after Restore • 24
Upgrade Issues • 72
Upgrading Clients • 45
Upgrading Legacy Clients • 45
Upgrading to Check Point Endpoint Security • 70
Upgrading to R80.10 Clients • 45
User Acquisition • 66
User Defined Report • 29
User Policy or Machine Policy • 50
Users Created at Installation • 15
Using CPInfo • 70
Using CPInfoPreboot • 71
Using Endpoint Security Administrator Console • 25
Using Program Advisor with a Proxy Server • 108

V
Versions in Use • 31
Viewing Assignments • 53
Viewing Endpoint Compliance Policy Assignments • 111
Viewing Full Disk Encryption Policy Assignments • 61
Viewing Malware Protection Assignments • 91
Viewing OneCheck User Settings Policy Assignments • 55
Viewing Program Advisor Recommendations • 107
Viewing Scheduled Tasks • 15

W
Wake On LAN • 65
WebCheck • 30, 118
Windows Integrated Logon • 64