Endpoint Security

Administrator Guide
Version NGX 7.0 GA

January 9, 2008
## Contents

**Preface**
- About this Guide ................................................................. 7
- Available Formats .............................................................. 7
- Obtaining the Correct Version .............................................. 8
- Obtaining Your Mode's Editions .......................................... 8
- Obtaining New Issues of this Guide ..................................... 8
- About the Endpoint Security Documentation Set .................. 9
- Documentation for Administrators ....................................... 9
- Documentation for Endpoint Users ...................................... 10
- Feedback ............................................................................ 10

**Chapter 1** 
### Introduction
- About Endpoint Security .................................................... 12
- Administering Endpoint Security ......................................... 12
- Integrations With Other Check Point Products ..................... 12
- What's New in this Release ............................................... 15
- Early Availability 1 ............................................................ 15
- Early Availability 2 ............................................................ 15

**Chapter 2** 
### General Workflow
- Administrator Workflow .................................................... 18

**Chapter 3** 
### Modes and Views
- Multi Domain Mode .......................................................... 22
- Single Domain Mode ......................................................... 23
- Simple View ..................................................................... 23
- Advanced View .................................................................. 24
- Switching Views .................................................................. 25

**Chapter 4** 
### Managing Administrators
- Introduction to Role-Based Administration ......................... 28
- Introduction to Administrator Assignment .......................... 29
- Introduction to Roles ....................................................... 29
- Default Roles and Customized Roles ................................. 29
- Privileges ......................................................................... 29
- SmartCenter Administrators ............................................. 30
- Planning your Administrator Configuration ....................... 31
- Administrator Account Workflow ...................................... 32
- Managing Administrator Accounts and Roles ..................... 33
- Creating Administrator Accounts ...................................... 33
- Editing Administrator Accounts ........................................ 34
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Security Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction to Security Policies ..................... 37</td>
</tr>
<tr>
<td></td>
<td>Enterprise Policies ........................................ 37</td>
</tr>
<tr>
<td></td>
<td>Personal Policies ........................................... 38</td>
</tr>
<tr>
<td></td>
<td>Policy Arbitration .......................................... 39</td>
</tr>
<tr>
<td></td>
<td>Policy Packages ............................................. 39</td>
</tr>
<tr>
<td></td>
<td>Security Policy Component Overview ................... 40</td>
</tr>
<tr>
<td></td>
<td>Firewall Rules ................................................ 40</td>
</tr>
<tr>
<td></td>
<td>Zone Rules .................................................... 40</td>
</tr>
<tr>
<td></td>
<td>Program Control ............................................... 40</td>
</tr>
<tr>
<td></td>
<td>Antispyware ................................................... 41</td>
</tr>
<tr>
<td></td>
<td>Antivirus ....................................................... 41</td>
</tr>
<tr>
<td></td>
<td>SmartDefense .................................................. 41</td>
</tr>
<tr>
<td></td>
<td>Mail Protections ............................................... 41</td>
</tr>
<tr>
<td></td>
<td>Enforcement Rules ........................................... 41</td>
</tr>
<tr>
<td></td>
<td>Policy Objects ................................................ 42</td>
</tr>
<tr>
<td></td>
<td>Rule Evaluation and Precedence ........................... 43</td>
</tr>
<tr>
<td></td>
<td>How Traffic is Evaluated .................................... 43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Managing Security Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prerequisites ................... 47</td>
</tr>
<tr>
<td></td>
<td>Policy Workflow ................. 48</td>
</tr>
<tr>
<td></td>
<td>Creating Policies ............... 49</td>
</tr>
<tr>
<td></td>
<td>Deploying Policies .............. 49</td>
</tr>
<tr>
<td></td>
<td>Configuring Office Awareness .... 50</td>
</tr>
<tr>
<td></td>
<td>Activating Policies ............. 51</td>
</tr>
<tr>
<td></td>
<td>Using a Default Policy .......... 52</td>
</tr>
<tr>
<td></td>
<td>Using a Default VPN Policy ...... 53</td>
</tr>
<tr>
<td></td>
<td>Managing Policy Versions ....... 54</td>
</tr>
<tr>
<td></td>
<td>Exporting Policies ................ 54</td>
</tr>
<tr>
<td></td>
<td>Deleting Policies ............... 55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Zone-Based Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction to Access Zones and Zone Rules ............ 57</td>
</tr>
<tr>
<td></td>
<td>Introduction to Zones ....................................... 57</td>
</tr>
<tr>
<td></td>
<td>Introduction to Zone Rules ................................ 58</td>
</tr>
<tr>
<td></td>
<td>Workflow for Zone-Based Security ........................ 59</td>
</tr>
<tr>
<td></td>
<td>Managing Zone-Based Security ............................ 60</td>
</tr>
<tr>
<td></td>
<td>Configuring New Network Detection Options ............. 60</td>
</tr>
<tr>
<td></td>
<td>Defining Zones ............................................... 60</td>
</tr>
<tr>
<td></td>
<td>Setting Security Levels .................................... 61</td>
</tr>
</tbody>
</table>
Chapter 8  Firewall Rules

Introduction to Firewall Rules .................................................. 63
Firewall Rule Rank in Security Policies ............................... 63
Firewall Rule Workflow ......................................................... 65
Managing Firewall Rules .......................................................... 66
Creating Firewall Rules ......................................................... 66
Adding Firewall Rules to Policies ............................................... 66
Ranking Firewall Rules ............................................................ 67
Enabling and Disabling Firewall Rules ......................................... 67
Editing Firewall Rules .............................................................. 68
Removing Firewall Rules from a Policy ......................................... 68
Deleting a Firewall Rule ........................................................... 68

Chapter 9  Program Control

Introduction to Program Control ............................................... 70
Program Permissions .............................................................. 70
Program Groups ................................................................. 71
Permission Precedence ............................................................ 72
Global and Policy Permissions ................................................ 72
Program Evaluation Process .................................................... 72
Using Checksums ................................................................. 73
Program Control Workflow ....................................................... 74
Planning Program Control ...................................................... 75
Managing Program Control ...................................................... 80
Creating Appscans ............................................................... 80
Adding Programs Manually ..................................................... 83
Creating Program Groups ...................................................... 84
Setting Program Permissions ................................................... 84
Setting Policy-Level Permissions ............................................. 85
Configuring Alert Levels ........................................................ 86

Chapter 10  Program Advisor

Introduction to the Program Advisor Server ............................... 88
Introduction to the Program Advisor Process ............................. 89
Program Advisor Workflow .................................................... 93
Managing Program Advisor .................................................... 94
Enabling Program Advisor ...................................................... 94
Viewing Program Advisor Recommendations ............................ 94
Overriding Program Advisor Recommendations ........................ 95
Managing Unknown Programs .................................................. 96

Chapter 11  Enforcing Endpoint Security

Introduction to Enforcement Rules ........................................... 98
Enforcement Rule Types ........................................................ 98
Preface

In This Preface

About this Guide


Before using this document to administer Endpoint Security, you should read and understand the information in the Endpoint Security Implementation Guide in order to familiarize yourself with the basic features and principles.

The features that are available to you in the Endpoint Security Administrator Console will depend on your role. See “Introduction to Role-Based Administration,” on page 28, and “General Workflow,” on page 17, for information about your role and its associated tasks. Use the workflow to identify the chapters of this guide that apply to your tasks. This document contains information that applies both to administrators who are tasked with the general configuration and administration of Endpoint Security, as well as those who are responsible for the implementation of security policies.

Available Formats

This guide is available in two formats:

- **Online Help** - This Guide is available in HTML format via topical links in the Endpoint Security Administrator Console Online Help.
- **PDF** - The PDF format of this document is available from the Check Point CD. Use the PDF format when you want to print this document. Updated editions of the PDF document may be available on the Check Point Website after the release of Endpoint Security.
Security. The PDF version of this document may be more up-to-date than the online version or the version on the CD.

When obtaining updated PDF editions from the Check Point Website, make sure they are for the same server version and mode as your Endpoint Security server. Do not attempt to administer Endpoint Security using documentation that is for another version or mode.

Obtaining the Correct Version

If you are using the PDF format of this document, make sure that it has the server version number that corresponds to the version of your Endpoint Security server. The server version number is printed on the cover page of this document. You can obtain your server number on the About page of the Endpoint Security Administrator Console.

Obtaining Your Mode's Editions

This document is available in Multi Domain, Single Domain, and Simple Mode editions. Always use the edition appropriate to your installation. All editions are available in PDF format from the Check Point User Center Web site or from the CD.

Obtaining New Issues of this Guide

New issues of this guide are occasionally available in PDF format from the Check Point Website. When using the PDF version of this document, make sure you have the most up-to-date issue available. The issued date is on the cover page of this document.

When obtaining the most up-to-date issue of the documentation, make sure that you are obtaining the issue that is for the appropriate server. Also make sure that you have the right edition for your mode.
About the Endpoint Security Documentation Set

A comprehensive set of documentation is available for Endpoint Security, including the documentation for the clients. This includes:

- “Documentation for Administrators,” on page 9
- “Documentation for Endpoint Users,” on page 10

Documentation for Administrators

The following documentation is intended for use by Endpoint Security administrators.

<table>
<thead>
<tr>
<th>Table 2-1: Server Documentation for Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td>Endpoint Security Installation Guide</td>
</tr>
<tr>
<td>Endpoint Security Administrator Guide</td>
</tr>
<tr>
<td>Endpoint Security Administrator Online Help</td>
</tr>
<tr>
<td>Endpoint Security System Requirements</td>
</tr>
<tr>
<td>Endpoint Security Gateway Integration Guide</td>
</tr>
<tr>
<td>Endpoint Security Client Management Guide</td>
</tr>
<tr>
<td>Endpoint Security Agent for Linux Installation and Configuration Guide</td>
</tr>
<tr>
<td>Endpoint Security Agent for Linux Installation and Configuration Guide</td>
</tr>
</tbody>
</table>
Documentation for Endpoint Users

Although this documentation is written for endpoint users, Administrators should be familiar with it to help them to understand the clients and how the policies they create impact the user experience.

Table 2-2: Client documentation for endpoint users

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Guide for Endpoint Security Client Software</td>
<td>Provides task-oriented information about the Endpoint Security clients (Agent and Flex) as well as information about the user interface.</td>
</tr>
<tr>
<td>Introduction to Flex</td>
<td>Provides basic information to familiarize new users with Endpoint Security Flex. This document is intended to be customized by an Administrator before distribution. See the Endpoint Security Implementation Guide for more information.</td>
</tr>
<tr>
<td>Introduction to Agent</td>
<td>Provides basic information to familiarize new users with Agent. This document is intended to be customized by an Administrator before distribution. See the Endpoint Security Implementation Guide for more information.</td>
</tr>
</tbody>
</table>

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com
Chapter 1
Introduction

In This Chapter

- About Endpoint Security  page 12
- What's New in this Release  page 15
About Endpoint Security

Endpoint Security allows you to centrally manage endpoint security functions for your enterprise. Endpoint Security is integrated with other Check Point products to allow you to manage all of your security together.

The major Endpoint Security features include:

- **Firewall Rules** – Provides same level of security as standard perimeter firewalls by restricting or allowing network activity based on connection information.
- **Access Zones and Zone Rules** – Provides network security through creating groups of locations to which you assign network permissions.
- **Program Control** – Restricts network access on a per-application basis.
- **SmartDefense Program Advisor Service** – Automates application control management.
- **Program Enforcement** – Ensures that every endpoint computer meets application and version requirements before it connects to the network. For example, using Program Enforcement, you can require that endpoint computers have a certain version of antivirus protection.
- **Cooperative Enforcement®** – Restricts or disconnects noncompliant users at the network access/authorization level. For a complete list of devices that are compatible with Endpoint Security, see the Endpoint Security Systems Requirements Guide.
- **Check Point Antispyware** – Protects your company's data by detecting and removing spyware.
- **Check Point Antivirus** - Provides centrally-managed antivirus protection to your endpoint users.

Administering Endpoint Security

Most administrative functions are performed using the Endpoint Security Administrator Console. The Endpoint Security Administrator Console is a Web-based graphical user interface and is available at http://<Endpoint Security IP Address>/signon.do.

Integrations With Other Check Point Products

Endpoint Security integrates with a variety of Check Point products to create an integrated security solution.

Notable integration points include:

- **Installation Options** – There are a variety of installation options for Endpoint Security with other Check Point products. These options include:
  - Single Server – You can now install Endpoint Security on the same server as SmartCenter and Provider-1. This reduces your resource costs.
- Multi-Server – You can install SmartCenter and Endpoint Security on separate servers. You can also choose to have logging on another server.

- Licensing – Licensing is performed on the server side so you do not need to update your Endpoint Security clients with a new license when adding features. You can manage your licenses using Check Point license management tools: SmartUpdate, the cplic command, or (for local licenses only) the Check Point Configuration Tool. See the Endpoint Security Installation Guide for more information about licensing.

- Gateway Integration – Endpoint Security provides Cooperative Enforcement in conjunction with the following Check Point devices and software:
  - Check Point VPN-1 for remote access users
  - Check Point VPN-1 UTM/Power
  - Check Point VPN-1® SecureClient™ with Application Intelligence
  - Check Point Interspect Gateway

  For supported versions, see the Endpoint Security System Requirements document. For information about integrating Endpoint Security with these devices, see “Introduction to Cooperative Enforcement,” on page 149.

- Unified Logging, Reporting, and Monitoring – Endpoint Security logs are stored in a format that makes them readable by third party and Check Point Products, such as SmartView Tracker, Eventia Reporter and Eventia Analyzer. This has the following advantages:
  - Logs use a file system instead of a database, which allows you to archive and rotate the logs in the same way as other Check Point logs.
  - Log info is stored locally if the remote logging server is unavailable.
  - Perimeter, internal, and Web Security events are all logged in one place.
  - Using Eventia Reporter you can schedule reports to run during periods of low system use. You can also e-mail reports to other people, and upload reports to a Web site.
  - Using SmartView Tracker, you can view logs in real time using a thick client application. The client application provides easy log navigation and filtering.
  - Certain reports in SmartPortal are available from the Endpoint Security Administrator console. See “Monitoring Client Security,” on page 172. This allows you to view the detailed reports you are interested in directly from the Endpoint Security Administrator Console.
  - SmartView Monitor displays real time Endpoint Security statistics, along with all other Check Point events.

- Shared Administrator Logins – You can use the same login for Endpoint Security as you do for other Check Point products. SmartDashboard automatically creates an Integrity object upon installation and grants Endpoint Security access to all administrators with SmartDashboard access.
Administrator accounts created in SmartCenter can launch Endpoint Security using the same read/write privileges assigned to them in SmartCenter. However, these administrators are not able to create administrator accounts in Endpoint Security. Also, you cannot create administrator accounts in SmartCenter using the roles and role permissions available in Endpoint Security (Examples: an account with the ability to assign policy, but not edit policies or an account with only the ability to run reports). To create these types of accounts you must log directly into Endpoint Security using the masteradmin login.
What's New in this Release

The following features are new in this release:

**Early Availability 1**

- **SecureClient Integration** - SecureClient is now fully integrated with Endpoint Security. You can now configure VPN access using the Endpoint Security Administrator Console to create a client package that allows VPN. For more information see “VPN Options,” on page 158.

- **Check Point Antivirus** - Check Point Antivirus provides centrally-managed antivirus protection to your endpoint users. For more information, see “Protecting Against Viruses,” on page 126.

- **Smart Defense** - SmartDefense provides your enterprise with protection from network attacks that exploit allowed traffic types. For more information, see “Using SmartDefense,” on page 142.

- **Improved Datastore** - Endpoint Security now uses an internal datastore that is easy to back up and restore.

- **Usability Enhancements and Simple View** - The Endpoint Security Administrator Console has been redesigned to enhance usability. There is also a new Simple View, to help administrators learn the basic Endpoint Security features. For more information about Simple View, see “Simple View,” on page 23.

**Early Availability 2**

- **High Availability** - Using Standby Servers, you can achieve a simplified Fail-over Configuration. You do not need an external load balancer or external Database failover. For information about configuring High Availability, see the Endpoint Security Installation Guide.

- **Office Awareness** - Through the use of the Office Awareness feature, the client is able to tell whether or not the endpoint computer is connected to your network. For more information about Office Awareness, see “Configuring Office Awareness,” on page 50.

- **Register to Hotspot Option for End-Users** - The Hotspot Registration feature makes temporary access possible for the endpoint user, while maximizing security by controlling the parameters of hotspot-specific port openings. Regardless of the restrictiveness of a policy, you can allow a temporary, controlled opening by selecting the Enable Hotspot Registration option in the policy. See “Allowing Endpoint Hotspot Registration,” on page 183.

- **Partial Client Updates** - When components of the client need to be updated, the client is able to install only the component that needs to be updated. Resolved Issues and Enhancements

- **Server Upgrades** - Automatic upgrades are available for installations of Endpoint Security NGX (R65 CD). Upgrades from versions earlier than Endpoint Security
NGX require a manual export of policies before upgrade, and then an import of those policies back following the upgrade. This import also imports some of the policy reference objects. For more information about upgrades, see the Installation guide.

- **General issues** - Cobra includes a number of resolved issues and additional enhancements based on feature requests and customer feedback, including:
  - Times are now reported in local time not GMT
  - Heartbeat and Web admin ports on the server are now different
  - Expanded unified security management and reporting
  - Faster switching between connected/disconnected policies on the client
  - Check Point licensing for the complete installation

For a complete list of resolved issues, see the Release Notes.
Chapter 2

General Workflow

Although some administrative tasks can be performed in any order, it is recommended that you use the general workflow given in this section as a guideline when working with your Endpoint Security system. Use the workflow to understand what tasks you should perform at what point, and to understand what resources are available to help you.

The workflow gives high-level information about the various tasks you may want to perform. More detailed information about these tasks are provided in other parts of this document, or in the other documents specified in the task.

The tasks you will perform will depend upon your role.
Administrator Workflow

1. Plan your installation.
   These prerequisite steps are essential to the success of your installation. Be sure to perform all of these steps before attempting to install or configure your Endpoint Security.
   a. Obtain all documentation.
      Make sure that you have the most up-to-date documentation and that it is the documentation that is appropriate for your version of Endpoint Security. See “About the Endpoint Security Documentation Set,” on page 9.
   b. Read the Release Notes.
      To prevent unexpected results familiarize yourself with the contents of the Endpoint Security Administrator Release Notes. Pay particular attention to any documentation issues listed in the readme in case any relevant instructions have changed.
   c. Check your requirements.
      Check the Systems Requirements document to verify that you have the right hardware and software for the Endpoint Security system. Check that any third-party products that you want to use, such as gateways or antivirus providers, are supported.
   d. Read the Implementation Guide and perform the pilot configuration steps.
      The Implementation Guide and the pilot will help you to plan your policies, your helpdesk training, and your endpoint user support. It also provides a basic introduction to important Endpoint Security features.
   e. If you plan to use Gateways or Microsoft GPO, make sure these are correctly configured and working perfectly before you attempt to use them with the Endpoint Security system.

2. Install and license the Endpoint Security
   a. Obtain your licenses.
      Endpoint Security is generally licensed according to how many client ‘seats’ you are allowed. Some add-on features, such as SmartDefense require additional licenses.
   b. Install the Endpoint Security server.
      There is a large variety of installation options for Endpoint Security. Use the Endpoint Security Installation Guide to Install Endpoint Security. During the installation, you will be prompted to choose whether you want to install the Single or Multi Domain Mode. See “Modes and Views,” on page 21 for more information about modes. You will also be prompted to enter your license information in SmartUpdate.
3. Perform your System Configuration.

Perform any system configuration task that you require, such as setting database backup options. For more information, see “Configuration and Maintenance,” on page 176.

4. Configure gateways and create catalogs.
   a. If you plan to use gateways with the Cooperative Enforcement feature of Endpoint Security, configure both your gateways and your Endpoint Security. See “Gateways and Cooperative Enforcement,” on page 148. You will also need the Endpoint Security Gateway Configuration Guide to perform this task.
   b. If you plan to use catalogs to allow you to assign policies to groups of endpoint users, create the catalogs and populate them with users. See “Introduction to Catalogs,” on page 32.

5. Create Roles and Administrator Accounts.

Define your Administrator roles and create accounts for your administrators. Each administrator will have roles that determine what the administrator can do. See “Creating Administrator Accounts,” on page 33.

6. Configure your global settings.

You can configure global settings for Program Control. These settings apply to your entire organization and are used in the policies by default.

7. Create and deploy policies.

Use policies to protect your network from security threats. Generally, you will manage your security policies using the Endpoint Security Administrator console.

For more information about basic security policy features and policy recommendations, see the Endpoint Security Implementation guide. For details on security policy features and task-oriented instructions, see the appropriate chapters in this guide. The following steps give an overview of some of the basic security features you may wish to configure:

Some of the features listed below may require the purchase of additional licenses.

   a. Protect against unauthorized network traffic to and from locations using Zone rules and firewall rules.


   b. Prevent unauthorized network traffic to and from programs using Program Control and Program Advisor.

      Use these features to restrict network access for programs and to terminate malicious applications. See “Program Control,” on page 69 and “Program Advisor,” on page 87.
c. Enforce Endpoint software requirements.
Use Enforcement rules to ensure that all the endpoint computers connecting to your network are adhering to your organization's security guidelines regarding required and prohibited software. See “Enforcing Endpoint Security,” on page 97.

d. Detect Viruses.
Use Check Point Antivirus to require antivirus scans on endpoint computers. See “Protecting Against Viruses,” on page 126.

e. Protect against malicious code in e-mail and enable attack protection.
Use Mailsafe to protect against worms and viruses spread through e-mail. See “Preventing E-mail Attacks,” on page 146. Use SmartDefense to protect against attacks that exploit allowed traffic. See “Introduction to SmartDefense,” on page 143.

f. Detect spyware.
Use Check Point Antispyware to require spyware scans on endpoint computers. See “Protecting Against Spyware,” on page 121.

8. Assign policies.
Assign policies to gateways, catalogs, and individual endpoint users to meet security needs. See “Assigning Policies,” on page 74

Deploy clients to endpoint computers. You can deploy clients using client packages or a number of third-party distribution methods. For more information about clients and client distribution, see the Endpoint Security Client Management Guide. For more information about Client Packages, see “Client Installation Packages,” on page 155.

10. Monitor and improve policies.
Use the reports to monitor the effectiveness of your policies. As needed, adjust your policies and redeploy them to your endpoint users. This system of monitoring and improving policies is known as a ‘policy lifecycle’. For more information about policy lifecycles, see the Endpoint Security Implementation Guide.
Chapter

Modes and Views

In This Chapter

Multi Domain Mode  page 22
Single Domain Mode  page 23
Switching Views  page 25

Use this chapter to understand how the modes and views of Endpoint Security work. If you, or another administrator, has already installed Endpoint Security, it will already be in one of these modes.

There are different versions of this document available for the different modes and views. Make sure that you are using the documentation that is appropriate to the mode and view you are using. The view you are using is displayed in the upper right corner of the Administrator console.
Multi Domain Mode

Use Multi Domain mode if you need to be able to create domains. You can use domains to organize users and policies into units. Each domain can have its own administrators and can be further divided into groups of endpoint users using catalogs. Multi Domain mode is particularly useful for Internet Service Providers and large companies that want local administration for business units or localities.

You can only configure Endpoint Security to operate in Multi Domain mode during installation. See the Endpoint Security installation guide for information about configuring this option and see “Switching Views,” on page 25 for an overview of the process.
Single Domain Mode

Use Single Domain mode if you do not need to organize your users and policies into units. In Single Domain mode there is only one domain, but it can be divided into groups of endpoint users to allow you to have different policies for different groups.

You can only configure Endpoint Security to operate in Single Domain mode during installation. See the Endpoint Security Installation Guide for information about configuring this option and see “Switching Views,” on page 25 for an overview of the process.

Single Domain has the following views:
- Simple - See “Simple View,” on page 23.
- Advanced - See “Advanced View,” on page 24

Simple View

Endpoint Security is very flexible, and, as a result, can be quite complex. While some administrators will need to use all the features, many situations require only the core Endpoint Security features. Use Simple view when you need only one domain, and do not immediately need all the features of Endpoint Security. Simple view is only available in Single Domain installations.

This document is intended for administrators using Simple view.

If you choose Single Domain during installation, it automatically starts out in simple view. After installation, use the General Settings page to toggle Simple view on or off. See “Switching Views,” on page 25.

Use Cases

Simple view can be useful under the following circumstances:
- Demonstrations - Use Simple view when you need to show core Endpoint Security functionality.
- Getting Started - Use Simple view to learn core functionality, then switch to regular Single Domain mode when you have mastered these basic steps.
- Simple Installations - If you do not need the advanced features of Endpoint Security, you can remain permanently in Simple view.

Simplified Features

Simple view provides an easier user interfaces for the following tasks:
- Creating Policies - Policies are always created through a Wizard that guides you through the process. “Creating Policies with the Policy Wizard,” on page 49.
- Activating Policies - Rather than assigning policies to users, in Simple view you just specify which policies you want to activate. See “Activating Policies,” on page 51.
Advanced View

Advanced view in Single Domain mode gives you access to all the Endpoint Security features, including features not included in Simple view:

- Domains
- Catalogs
- Policy assignment
- Policy creation from templates or files
- Manually-added reference sources for programs
- Server settings

If you need to use these features in Single Domain mode, switch to Advanced View. See “Switching Views,” on page 25. Multi Domain installations are always in Advanced View.
**Switching Views**

You must choose Multi or Single Domain mode when you install Endpoint Security. If you choose to install the Single Domain mode, it automatically starts in Simple view.

After installation, you can switch between Advanced and Simple views using the Administrator Console. "Choosing Modes and Switching Views," on page 25 shows the process.

Figure 3-1: Choosing Modes and Switching Views

1. The Endpoint Security Installation Wizard runs.

   The Endpoint Security Installation Wizard helps you to perform the initial installation and configuration of your system. It prompts you to choose Single or Multi Domain Mode. For more information about the Installation Wizard and choosing modes, see the Endpoint Security Installation Guide.
2. If you choose Multi Domain, when the Installation Wizard is finished, Endpoint Security starts in Multi Domain mode. You cannot switch modes after installation.

3. If you choose Single Domain mode, Endpoint Security starts in Simple view.

4. After installation, you can optionally choose to change to Advanced view. You may decide to switch to Advanced view after you have become familiar with basic Endpoint Security features, or when you need the more advanced features, such as policy assignment.

5. You can switch from Advanced to Simple view at any time, provided you have not used any of the features that are not included in Simple view.

**To switch between views:**

1. At the top of the Endpoint Security Administrator console, click **Change View**. The Confirm Change View page appears.

2. Click **Change View**.
Chapter 4
Managing Administrators

In This Chapter
- Introduction to Role-Based Administration
- Introduction to Administrator Assignment
- Introduction to Roles
- SmartCenter Administrators
- Planning your Administrator Configuration
- Administrator Account Workflow
- Managing Administrator Accounts and Roles
Introduction to Role-Based Administration

Endpoint Security provides extremely flexible administration capabilities. You can create administrator accounts that are limited to specific user sets. You can also create accounts that can only perform specific functions. This lets you configure administrator accounts that correspond to the division of responsibilities within your organization.

Administrators are usually responsible for the following tasks:

- Creating and assigning security policies
- Monitoring connections and running reports on client activity
- Troubleshooting endpoint user connection issues
Introduction to Administrator Assignment

An administrator’s assignment determines which parts of your organization he or she administers.

Introduction to Roles

Each administrator must be assigned a role. Roles are composed of privileges, which determine the Endpoint Security features the administrator can access.

Use roles as a convenient way to assign a set of privileges to administrators.

If you cannot find a particular feature in the Endpoint Security Administration Console, your assigned role does not have the privileges for that feature.

Default Roles and Customized Roles

Endpoint Security comes with several pre-configured roles for your convenience. These roles are designed to reflect the most common division of administrative tasks. Use the Role Manager page to view the available pre-configured roles. For navigation information see “Role Manager,” on page 194.

If the default roles reflect the administrative responsibilities in your organization, you can simply assign one of these roles to each of your Endpoint Security administrators.

If the default roles do not reflect the administrative responsibilities in your organization, you can edit them or you can create new, customized roles. You may want to use a default role as a template for your customized role.

Privileges

Privileges consist of a set of read/write permissions for various Endpoint Security features.

For each privilege, there are three possible permission settings:

- **No access** - The administrator cannot access the feature. All links to the feature are hidden.
- **Read** - The administrator can view the feature, but cannot change any settings or perform actions. Controls, such as check boxes and command buttons, do not appear, and Endpoint Security displays only navigation buttons.
- **Read/Write** - The administrator can access the feature change settings.

To see the privileges for a role, see the Role page. For navigation information, see “Role,” on page 194.
SmartCenter Administrators

Administrator accounts created in SmartCenter can launch Endpoint Security using the same read/write privileges assigned to them in SmartCenter. However, these administrators are not able to create administrator accounts in Endpoint Security. Also, you cannot create administrator accounts in SmartCenter using the roles and privileges available in Endpoint Security. To create these types of accounts you must log directly into Endpoint Security using the masteradmin login.
Planning your Administrator Configuration

Before you begin configuring your administrators and their roles, you need to know the following:

- The e-mail addresses of all your administrators.
- The roles and privileges you want your administrators to have.
- Whether you want to restrict administrator access to a particular catalog, gateway, or group.
- Whether you want to use RADIUS authentication or Endpoint Security’s built-in authentication.
Administrator Account Workflow

Although it is possible to perform many of the administrator account tasks in any order, it is recommended that you use the following workflow as a guide.

To configure your administrator accounts:

1. Plan your administrator configuration.
   See “Planning your Administrator Configuration,” on page 31.

2. Configure RADIUS administrator authentication. (Optional)
   If you want to use a RADIUS server to authenticate your administrators, configure it now. See “Configuring a RADIUS Server,” on page 186.

3. Create your administrator accounts.
   Depending on your needs, you may also need to:
   a. Assign roles.
      If you want your administrators to have only the permissions appropriate to their jobs, assign them roles. You can use the preconfigured roles provided with Endpoint Security or create your own. See “Creating Roles,” on page 35.
   b. Assign entities.
      If you want your administrators to be assigned to certain catalogs or gateways, assign them to entities.

4. Distribute information to your administrators.
   Send the administrators the login and password information for their accounts. You should also include the URL of the Endpoint Security server login page.
   If you are using RADIUS authentication for your administrators you will only need to send them the login URL. RADIUS-authenticated administrators will use their RADIUS logins and passwords.
Managing Administrator Accounts and Roles

This section contains the following topics.
- “Creating Administrator Accounts,” on page 33
- “Editing Administrator Accounts,” on page 34
- “Deleting Administrator Accounts,” on page 34
- “Creating Roles,” on page 35
- “Editing Roles,” on page 35
- “Deleting Roles,” on page 35

Creating Administrator Accounts

Before you create administrator accounts, you should know the answers to the following questions:

- What is the administrator’s log in ID and e-mail address?
  
  If the Endpoint Security administrators are authenticated against an external database, the administrator ID must match the user name in the external database.

  If external administrator accounts are in different catalogs and administrators can have the same name, append the catalog name before the user name as follows: `catalog.username`.

- Which role do you want to assign to the administrator?
  
  When you create the account, you must assign the role. You can create the roles that you need in advance, using the Role Manager page, or you can create them as you need them while creating administrator accounts.

- Which entities do you want the administrator to manage?
  
  You can assign the administrator to one or more specific catalogs or groups. Administrators that are not assigned to a catalog or group are assigned to the entire organization by default.

Use the Endpoint Security Administrator Console to create administrator accounts.

To create an administrator account:

1. Go to the Administrator Manager page.
   
   For navigation information, see “Administrator Manager," on page 191.

2. Click New.

3. Complete the information for the administrator.
   
   If you are not using RADIUS authentication, be sure to record the username and password you set for your administrator. You will later need to send this information
to your administrator. For more information about completing the administrator information, see the Endpoint Security online help.

4. Assign a role to the administrator.
   a. In the Assigned Role area, click Edit.
   b. Select the role, and click Assign.
      If you need to create a new role, see “Creating Roles,” on page 35.

5. If you want to restrict the administrator’s ability to assign policies to users, assign the administrator to the catalog, group, or gateway. Administrators that are assigned to a catalog, group, or gateway are able to assign policies only to members of that catalog, group, or gateway. Administrators that are not assigned to a catalog or group are assigned to the entire organization by default.
   a. In the Assigned Catalog area, click Edit.
   b. Select the catalog or group and click Assign.

6. Click Save.

**Editing Administrator Accounts**

You can make changes to administrator accounts using the Administrator Manager page in the Endpoint Security Administrator Console. For navigation information, see “Administrator Manager,” on page 191.

Note the following when editing administrator accounts:

- To make changes to an administrator account, your role must have privileges equal to or greater than the role of the account you want to change.
- You can change the user catalogs and groups an administrator has access to by editing the administrator account.
- If you change role assignment or privileges, Administrators receive the modified role the next time they log on.

**Deleting Administrator Accounts**

You can delete administrator accounts using the Administrator Manager page in the Endpoint Security Administrator Console. For navigation information, see “Administrator Manager,” on page 191.

Note the following when deleting administrator accounts:

- If administrators are logged on when you remove their accounts, they are automatically logged off.
Creating Roles

You can create a new role by duplicating an existing role on the Role Manager page and then making edits, or by defining an entirely new role.

To create a role:

1. Go to the Role Manager page.
   For navigation information, see “Role Manager,” on page 194.
2. If you want to copy an existing role, click Duplicate, if you want to create a completely new role, click New.
3. In the Access Privileges area, select the read/write permissions you want.
   You cannot create a role with greater privileges than your own. Endpoint Security does not display privileges for which you have insufficient permission.
4. Click Save.
   You can now assign this role to administrators.

Editing Roles

You can edit roles using the Role Manager page in the Endpoint Security Administrator Console. For navigation information, see “Role Manager,” on page 194.

Endpoint Security applies the changes the next time the administrator logs on.

Deleting Roles

You can delete roles using the Role Manager page in the Endpoint Security Administrator Console. For navigation information, see “Role Manager,” on page 194.

You cannot delete a role that is currently assigned to an administrator. You must reassign all the administrators to a new role before you can delete the role.
Chapter 5
Security Policies

In This Chapter

Introduction to Security Policies ........................................... page 37
Security Policy Component Overview ................................. page 40
Policy Objects ........................................................................................................ page 42
Rule Evaluation and Precedence ........................................ page 43

Creating security policies is the core task involved in implementing security with Endpoint Security. Use this chapter to:

■ Understand the types of security policies that are available.
■ Get an overview of the components that are used in security policies.
■ Understand the order in which Endpoint Security enforces the rules you establish in your security policies.
Introduction to Security Policies

An Endpoint Security security policy is a set of rules and settings that governs the behavior of your endpoint computers. Use Endpoint Security security policies to achieve the goals of your organization's security regulations.

Administrators create enterprise policies using the Administrator Console and assign them to endpoint users or groups of endpoint users. Endpoint Security deploys these enterprise policies to endpoint computers, where the clients receive and enforce them. For more information about the policy workflow, see “Policy Workflow,” on page 48.

There are the following types of policies:

- Enterprise Policies
- Personal Policies

Enterprise Policies

Enterprise policies provide centralized management of your endpoint security. Administrators create enterprise policies and assign them to endpoints.

Depending on your organization's security needs, you may wish to enforce different policies when endpoints are connected or disconnected from your network. To do this, define your policies and then designate them as the connected or disconnected policies.

Policies are not designated as 'connected' or 'disconnected' when you create them. Any policy can serve as a connected or disconnected policy depending on how it is activated.

Connected Policies

The connected enterprise policy is the policy that is enforced when the endpoint computer is connected to the Endpoint Security server. Generally, this is a fairly restrictive policy. 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 policies. For example, a connected policy might require more restrictive firewall rules, require a particular antivirus program, or block programs that violate your company's ethics policies, such as illegal file sharing programs.

Disconnected Policies

The disconnected enterprise policy is enforced when the endpoint computer is not connected to your network. Sometimes this policy is less restrictive, but provides a minimum level of security that you can then depend upon at all times. In other implementation, you may want this policy to be more restrictive to prevent recreational use of endpoint computers.
Through the use of the Office Awareness feature, the client is able to tell whether or not the endpoint computer is connected to your network. For more information about Office Awareness, see “Configuring Office Awareness,” on page 50.

If you do not configure Office Awareness, your clients will use the disconnected policy whenever they lose contact with the Endpoint Security server. The use of Office Awareness is highly recommended when using disconnected policies.

When the endpoint computer is not connected to your network, the connected policy is deactivated and the disconnected policy comes into effect. The connected policy continues to try to connect to your network. The disconnected policy doesn’t send heartbeats. Once the connected policy successfully connects to the network, it comes back into effect and disables the disconnected policy.

The goal of the disconnected policy is usually to protect the endpoint computer from the worst threats while allowing the user more freedom. For example, a disconnected policy might require that the endpoint have antivirus protection, but not be as strict about which brand or version. It might also allow users to run entertainment programs that they are not allowed to run while connected.

If you do not want to control an endpoint computer’s security when it is disconnected, you can omit the disconnected policy. In the case of Flex users, the personal policy is enforced in the absence of a disconnected policy.

Windows versions of Flex and Agent can use disconnected policies. If you deploy a policy package to an Agent for Linux, the disconnected policy within the policy package will be ignored. Agent for Linux will only take the connected enterprise policy. Use the RPM Package builder to configure a disconnected policy for Agent for Linux. For more information, see the Agent for Linux Installation and Administration Guide.

**Personal Policies**

Flex users can create their own security policies. These policies are known as ‘personal policies’. The personal policy gives some control over security management to the endpoint user, who defines the policy using the Flex Control Center (user interface).

Agent users do not have access to personal policy settings, although Agent does include an ‘empty’ personal policy accessible only through a configuration file.

How these policies are arbitrated with conflicting enterprise policies depends on what settings you choose in the enterprise policy. Generally, the more restrictive policy rule is the one that is enforced.

The personal policy is installed with the client by default. You can specify a pre-configured personal policy using the client packager or the client parameters, depending on your client deployment method. For more information about the client packager, see “Client Installation Packages,” on page 155. For more information about client parameters, see the Endpoint Security Client Management Guide.
If you do not specify an enterprise policy when deploying the client, the client enforces the personal policy until it receives an enterprise policy to override the personal policy.

**Policy Arbitration**

Flex arbitrates between conflicting personal policy and enterprise policy settings. Configure arbitration options in all enterprise policies that you plan to assign to endpoint users that are using Flex. Unless you specify otherwise, the more restrictive policy rule is the one that is enforced.

For example, if the enterprise policy is configured to allow inbound traffic on port 135, but the personal policy is configured to block it, the traffic will be blocked. Such traffic will also be blocked if the personal policy is configured to allow it, and the enterprise policy is configured to block it.

Configure your policy arbitration options in the enterprise policy. Arbitration options are set in the Client Settings page. The following arbitration options are available:

- Permit or prevent the user from shutting down the client when the enterprise policy is active.
- Enforce only the enterprise policy, ignoring personal policy settings.

If you choose to ignore personal policy settings, it is highly recommended that you also select the option to warn endpoint users that their settings will not be enforced. Otherwise the endpoint users will not understand why their security settings have no effect.

**Policy Packages**

Policy packages are bundles of policies that can be assigned together. Using packages, you can indicate which policy to enforce as the connected policy and which to enforce as the disconnected policy.

Policy arbitration rules for policy packages are the same as policy arbitration rules for unpackaged enterprise policies. However, policy arbitration rules are enforced after the connection state determines which enterprise policy is enforced. Then the enforced enterprise policy is arbitrated with the personal policy.
Security Policy Component Overview

Enterprise and personal policies consist of various types of security rules and settings. Before configuring security policies, it is important to understand these rules and how they are evaluated and enforced by clients.

This section briefly describes the types of security rules that make up enterprise and personal policies. For more detailed information about these features, see the Endpoint Security Implementation Guide and the appropriate chapters of this guide. Some features may require the purchase of additional licenses.

Firewall Rules

Firewall rules take a traditional perimeter firewall approach to securing the endpoint. Firewall rules block or allow network traffic based on attributes of communication packets. You can use firewall rules to block or allow traffic based on the following attributes:

- Source and/or destination locations
- Protocol and/or port
- Time and/or day activities occurs

For more information, see “Firewall Rules,” on page 62.

Zone Rules

In addition to firewall rules, you can also control network traffic through the use of Access Zones and Zone Rules. Access Zones are groups of locations to which you assign the same network permissions. Zone Rules control network activity to and from your Zones. For more information, see “Zone-Based Security,” on page 56.

Program Control

Program rules restrict network access on a per-program basis. Whereas firewall rules restrict access according to package content, and Zone Rules according to location, Program Control allows you to restrict network access between a particular program and either your Trusted or Internet Zone. For more information, see “Program Control,” on page 69.

Program Advisor

Program Advisor is a service provided by Check Point that gives program permission recommendations for programs. 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 requires the purchase of an additional license. For more information, see “Program Advisor,” on page 87.
Antispysware

Check Point Antispysware protects your network from threats ranging from worms and Trojan horses to adware and keystroke loggers. Antispysware is a service Check Point provides to customers who purchase a separate Antispysware license. Endpoint Security regularly receives updated spyware definitions from the SmartDefense Antispysware Service, a central server maintained by Check Point. Administrators use these definitions in specific policies or in global Antispysware settings to enforce regular spyware scans and treatments on endpoints. For more information, see “Protecting Against Spyware,” on page 121.

Antivirus

Check Point Antivirus protects your endpoint users from known and unknown viruses by scanning for known viruses and for characteristics of viruses. You have the option of configuring the schedule, deploying the updates only after testing them, or even deploying the latest update immediately whenever necessary. When a virus is detected, the client can render it harmless, either by repairing or denying access to the infected file. For more information, see “Protecting Against Viruses,” on page 126.

SmartDefense

Activating SmartDefense on your endpoints protects your network from network attacks. These attacks are characterized by the misuse of allowed traffic and services. They have the capacity to slow or immobilize a network and cause Denial of Service (DoS) conditions that block endpoint access to hosts and servers. When SmartDefense protections are in place on your endpoints, the network is protected from attacks such as the Ping of Death, SQL Slammer, Tear Drop, HTTP worm, etc. Attempted attacks and treatments are also tracked and recorded for your observation. For more information, see “Using SmartDefense,” on page 142.

Mail Protections

Use Endpoint Security to protect against e-mail threats using Mailsafe. The Mailsafe feature puts limits on outgoing e-mail to prevent e-mail worms and other malicious code from using the endpoint computer to send messages.

Enforcement Rules

Use enforcement rules to ensure that protected computers comply with your security policies regarding antivirus and other types of software. If a protected computer does not comply with one or more enforcement rules, you can restrict the connection using restriction firewall rules.
Policy Objects

Policy objects are the interchangeable parts of your policies. You can use policy objects over and over again in different policies. The following are policy objects:

- Firewall Rules
- Locations
- Ports and Protocols
- Enforcement Rules

Once you create a policy object it is available for use in all your policies. You can create policy objects in the following ways:

- **In Advance** - You can use the Policy Objects page to create all, or most of your policy objects at once. This is useful when you first start your implementation and want to enter all your locations, ports, and protocols at once. For navigation information, see “Policy Objects,” on page 193.

- **As Needed** - You always have the opportunity to create policy objects as you need them while configuring your policies.
Rule Evaluation and Precedence

It is possible for a single policy to contain conflicting rules. For example, the same policy might contain a firewall rule that blocks incoming traffic on port 135, and a Zone rule that allows incoming traffic on that port. Therefore it is important to understand how the different rules are evaluated and enforced by the Endpoint Security client, and which rules take precedence if there is a conflict.

How Traffic is Evaluated

The Endpoint Security client checks hard-coded firewall rules before evaluating traffic against the enterprise or personal policy rules. Network traffic is evaluated the same way whether it is incoming or outgoing.

Hard-Coded Rules

Hard-Coded Rules are provided by Endpoint Security by default to facilitate traffic and help provide some basic security. These rules take precedence over rules in your policies and are not displayed in the Endpoint Security Administrator Console. You can manually reconfigure the following hard-coded rules by making changes to the XML policy file, but this is not recommended.

- Allow UDP (User Datagram Protocol) packets to and from the Endpoint Security port 6054
- Allow TCP packets to and from the Endpoint Security port 443
- Allow traffic from the local machine to port 53 on any computer
  - This rule allows access to the Domain Name Service.
- Accept ICMP (Internet Control Message Protocol) type 9 to local machine
  - This rule allows router advertisement.
- Block all traffic from sources which is not in the Trusted or the Internet Zone
  - This rule is the 'cleanup rule', which blocks all unhandled traffic.

Security Rules

Figure 5-1 shows how a client evaluates the security rules for network traffic.
The client checks hard-coded firewall rules before evaluating traffic against the enterprise or personal policy rules. If the traffic is allowed by the hard-coded rules, the client then verifies the traffic against the policy in the following order:

1. The client checks for a matching Firewall Rule.
   - If the Firewall Rule defined in the policy says to block this traffic, the traffic is blocked.
   - If there is no Firewall rule blocking this traffic, the evaluation process proceeds to the next step.

2. The client checks if the traffic is going to or coming from a restricted Zone.
   - If the traffic comes from, or is going to a Zone that is defined as restricted, the traffic is blocked.
   - If the traffic does not come from or going to a restricted Zone, the evaluation process proceeds to the next step.

3. The client checks for applicable program rules.
   a. If the traffic matches a program rule in the policy, the client applies that program rule.
b. If the traffic does not match any program rules, the client applies the Zone rule.
# Chapter 6

## Managing Security Policies

In This Chapter

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>page 47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Workflow</td>
<td>page 48</td>
</tr>
<tr>
<td>Using a Default VPN Policy</td>
<td>page 53</td>
</tr>
<tr>
<td>Managing Policy Versions</td>
<td>page 54</td>
</tr>
<tr>
<td>Exporting Policies</td>
<td>page 54</td>
</tr>
<tr>
<td>Deleting Policies</td>
<td>page 55</td>
</tr>
</tbody>
</table>

Use this chapter to understand the policy workflow and how to manage versions of your policies.
Prerequisites

Although some tasks can be done in any order, it is recommended that you follow the general task order given in “General Workflow,” on page 17. At a minimum, this chapter assumes you have:

- Created your catalogs and gateways.
- Read the Endpoint Security Implementation Guide and performed the pilot installation.
Policy Workflow

Perform the following steps to create your security policies and deliver them to your endpoint users.

1. Plan your policies.
   Before you begin, you should plan your policies. It is highly recommended that you iteratively create and deliver policies to your users to achieve your security goals. This process is called a ‘policy lifecycle’. For more information about planning policies and policy lifecycles, see the Endpoint Security Implementation Guide.

2. Create your policy objects (optional).
   You can create your policy objects (such as locations) as you need them in your policies, or you can create them all at once before you begin creating policies. Generally, administrators that are new to Endpoint Security will create policy objects as needed. More experienced administrators may prefer to create all or most of their objects before creating their policies using the following pages:
   - Firewall Rule Manager
   - Location Manager
   - Ports and Protocols Manager
   - Enforcement Rules Manager

3. Create your policies.
   Using the Endpoint Security Administrator Console, make your new policies and configure your security options. See “Creating Policies,” on page 49.
   If you do not want to create your own policies, you can use the pre-configured policy templates.

4. Deploy your policies.
   Deploying a policy makes the latest version of the policy available for download by clients. See “Deploying Policies,” on page 49.

5. Configure Office Awareness (recommended).
   If you are using disconnected policies, it is highly recommended that you use Office Awareness to ensure that the disconnected policy is only activated when endpoint computers are actually disconnected from your network. See “Configuring Office Awareness,” on page 50.

6. Assign your policy or policy package.
   Assignment is the way that a policy is associated with an endpoint user. You can assign policies and policy packages to:
   - Catalogs (such as user catalogs or IP ranges)
   - Gateways
   - Groups
Individual Endpoint Users

At this point your policies are assigned and available for clients to download on the next heartbeat or the next login. For information about distributing clients to endpoint computers see the Endpoint Security Client Management Guide.

Creating Policies

Create your policies. You can then bundle them into policy packages for your convenience.

Creating Policies with the Policy Wizard

The policy wizard provides an easy way for you to set up a simple policy.

To create a policy using the Policy Wizard:

1. Go to the Policy Manager page.
   For navigation information, see “Policy Manager,” on page 193.
2. Click New and select From Wizard.
   The policy wizard begins. Proceed through the pages of the wizard. For more information about security rules and settings, see the associated chapters in this guide and the online help.
3. Define the policy and click Next.
4. Define your Zones and click Next.
5. Set your basic protections and click Next.
   The policy wizard allows you to configure basic settings for:
   • Check Point Antivirus
   • Check Point Antispyware
   • Program Control
   • Outbound E-mail
6. Configure the alert text that your endpoint users will see and click Finish.
   Your policy is now available for download.
   If you have not already done so, you should deploy clients to your endpoint computers. For information about deploying clients see “Client Installation Packages,” on page 155, and the Endpoint Security Client Management Guide.

Deploying Policies

When you save a policy, Endpoint Security does not automatically deploy it. This lets you save cumulative changes to a policy without affecting users. It also lets you deploy
the policy when it is convenient for you (during off hours, for example, when users are not at work and more bandwidth is available).

**To deploy a policy:**

1. Go to the **Policy Manager** page.
   - For navigation information, see "Policy Manager," on page 193.
2. In the row for the policy, click **Deploy**.
   - A confirmation message appears.
3. Click **Yes**.
   - The policy is now available for endpoints to download. If you have already assigned the policy, the endpoints it is assigned to will download the policy on the next heartbeat or the next time they log in.

**Configuring Office Awareness**

Office Awareness allows the client to know whether the endpoint computer is connected to your network or not. Use Office Awareness to ensure that the disconnected policy becomes active only when the endpoint computers become disconnected from your network, not when they become disconnected from the Endpoint Security server. Office Awareness works by specifying Awareness Servers that are already on your network. As long as the endpoint computers remain in contact with the Office Awareness Servers, they will remain in connected mode and continue to use the connected policy. This helps to maintain the correct levels of security and user productivity, even if the Endpoint Security server becomes disabled or disconnected.

In order to have Office Awareness, a client must have synchronized with the Endpoint Security server and received the list of Office Awareness Servers. Because of this, Office Awareness may take some time to go into effect for all endpoint computers.

**Specifying Office Awareness Servers.**

Office Awareness Servers are servers that already exist on your network, such as DNS, DHCP, or Gateway servers. When you specify these servers as your Office Awareness Servers, the client uses them to determine whether or not the endpoint computer is connected to your network. If it cannot contact these servers, the client applies the disconnected policy.

This is the easiest method of providing office awareness. However, it is potentially vulnerable to spoofing. The risk of spoofing can be reduced by using the MAC address instead of the IP address of the servers.

In order for Office Awareness to function correctly, you must specify Office Awareness Servers that are already in use by your endpoint computers.
To specify Office Awareness Servers:
1. Go to the Client Configuration page.
   For navigation information, see “Client Configuration,” on page 191.
2. In the Office Awareness area, click Edit.
3. Add the servers you want to use.
   You can choose to require contact with all or any of the servers. Use the MAC
   address instead of the IP for additional security. For information for completing
   this page, see the online help.
4. Click Save.

Activating Policies

In simple mode, you cannot assign policies. Instead, you can choose which policies to
activate as your connected, disconnected, and gateway policies. Disconnected policies
apply to users that are not connected to the Endpoint Security server. Gateway policies
apply to users who connect through a gateway. The same policy applies for all the
gateways you have defined. Any other policies you have created remain inactive, and
do not affect your endpoint users.

To activate policies:
1. Click Policies.
2. In the Use As column for the policy, click Connected, Disconnected or Gateway.
   The policy is then in use.
Using a Default Policy

Check Point provides a pre-configured Default Policy. You can customize this policy to suit your organization's needs.

A copy of the Default Policy you create in the System Domain is inherited by all the Domains you create after defining it. This copy is known as the 'Default Domain Policy'. Domain Administrators can use the Default Domain Policy as you provide it, or make changes to it to customize it for their needs. The changes that Domain Administrators make to their copies of the Default Domain Policy do not affect the original Default Policy.

Users that do not belong to any Domain, catalog, or gateway are assigned the Default Policy by default.

To use the Default Policy:

1. Configure the Default Policy.
   The steps for configuring a default policy are generally the same as for any existing policy.
   a. Go to the Policy Manager page.
      For navigation information, see "Policy Manager," on page 193.
   b. Edit the Default Policy to meet your organization's needs.
      In the row for the Default Policy, click Edit and make any necessary changes to the policy.
   c. Deploy the Default Policy.
      See "Deploying Policies," on page 49.

2. Assign the Default Policy to unknowns.
   a. Go to the Domain Manager page.
      For navigation information, see "Domain Manager," on page 192.
   b. Go to the Endpoint Manager page.
      For navigation information, see "Endpoint Manager," on page 192.
Using a Default VPN Policy

The Endpoint Security server includes a Default VPN Policy for you to apply to VPN-1 gateways with minimal configuration. This policy is designed to keep out any incoming traffic that is not encrypted. It is also configured to allow encrypted outgoing traffic, SCV keep alive, and outgoing Visitor Mode traffic.

In order to take advantage of the Default VPN policy, the best practice is to duplicate it and then configure it to work with the VPN-1 gateway, as described in the workflow steps that follow.

**Visitor Mode** tunnels all client-to-gateway communication through a regular TCP connection on port 443. All required VPN connectivity (IKE, IPsec, and so on) between the client and the server is tunneled inside this TCP connection. This means that the peer gateway needs to run a Visitor Mode (TCP) server on port 443.

**Default VPN Policy Workflow**

Unlike the regular Default Policy, the Default VPN Policy is not applied automatically to any unassigned users. Instead, you configure it for your gateway and apply it to the gateway, as outlined in the steps that follow.

1. Make a duplication of the Default VPN Policy, which you will customize for your gateway.
   a. Go to the **Policy Manager** page. 
      For navigation information, see “Policy Manager,” on page 193.
   b. Under **Default VPN Policy**, click **Duplicate**.

2. Edit the SC firewall rules in order to add the VPN gateway:
   a. Go to the **Firewall Rule Manager**. For navigation information, see “Firewall Rule Manager,” on page 192.
   b. Add the VPN-1 gateway as **SC Outgoing** Destination.
   c. Add the VPN-1 gateway as **SC Incoming** Source.
   d. Add the VPN-1 gateway as the **SC Visitor Mode** Destination.

3. Add the gateway IP address to the **Trusted Zone** for this policy.
   See “Defining Zones,” on page 60 for information on creating policies and Trusted Zones.

4. Assign the VPN Policy to the VPN-1 gateway.
   See “Deploying Policies,” on page 49.

5. In order to allow clients to initially connect, do the following:
   a. Add the **SC Outgoing** firewall rule to the disconnected policy.
   b. Add the gateway IP address to the disconnected policy’s **Trusted Zone**.
Managing Policy Versions

Each time you save a policy, Endpoint Security stores a copy of the policy for reference and rollback. You can use the policy history rollback function to restore the settings of an earlier version of a policy.

Viewing the original policy version of a prepackaged policy is useful when you need to know the default values for a security setting.

When you roll back to a previous policy version, the policy uses current definitions for policy components, such as firewall rules and location definitions. Occasionally, the following conditions may occur when you roll back to an earlier version of a policy:

- The rule or definition was modified since you created that version of the policy. In this case, the policy includes the most current settings for rule or definition.
- The rule or definition was deleted since you created that version of the policy. In this case, the policy includes the original, deleted rule or definition. The deleted rule or definition becomes local to the policy. It does not appear in the Policy Objects pages and is not available for use in other policies.

To roll back a policy to a previous version:

1. Go to the Policy Manager page.
   For navigation information, see “Policy Manager,” on page 193.
2. In the row for the policy, click History.
3. To view the policy settings for the saved version, click the link in the Date Saved column.
4. Inspect the policy settings to verify that this is the version you want to restore and click Back.
5. In the version list, select a version, then click Roll Back.
   A confirmation message appears.
6. Click Yes.

After you have rolled back to a previous version, you must deploy the policy to send it to the assigned users.

Exporting Policies

You can export a policy for use with another Endpoint Security server.

To export a policy:

1. Go to the Policy Manager page.
   For navigation information, see “Policy Manager,” on page 193.
2. In the row for the policy, click Export.
   A dialog appears, asking you if you want to save the file.

3. Click Save.

4. Choose the location and name for your policy and click Save.
   The policy is saved as an XML file. You can import this policy into another
   Endpoint Security server by creating a new policy using the file.

Deleting Policies

You cannot delete a policy while it is assigned or is included in a client package.

To delete a policy:

1. Remove all policy assignments for the policy.
   a. Go to the Policy Manager page.
      For navigation information, see “Policy Manager,” on page 193.
   b. Select the policy, and click View Assignments.
      The Endpoint Manager page appears, showing only those catalogs that have
      your chosen policy assigned to them.
   c. Select the catalogs and select a new policy assignment from the Policy
      dropdown.
      You can either explicitly assign a different policy to the catalogs, or you can
      choose to have the catalog inherit the policy from its parent.
   d. Click Assign.
      Be sure to perform steps c-d for all the catalogs that are assigned the policy.

2. Remove the policy from all policy packages.
   a. Go to the Policy Manager page.
      For navigation information, see “Policy Manager,” on page 193.
   b. For all the policy packages (indicated by an icon), check the Description
      field for the policy you want to delete.
   c. For the policy packages that contain the policy you want to delete, click Edit
      and choose another policy for the package.
   d. Click Save.
      Be sure to perform steps c-d for all the policy packages that contain the policy you
      want to delete.

3. In the row for the policy, click Delete.
   A confirmation message appears.

4. Click Yes.
Chapter 7

Zone-Based Security

In This Chapter

Introduction to Access Zones and Zone Rules page 57
Workflow for Zone-Based Security page 59
Managing Zone-Based Security page 60

This chapter explains how to use the Endpoint Security's Access Zones and Zone rules features to create security rules in policies that control protected endpoint computer network activity.
Introduction to Access Zones and Zone Rules

Zone rules allow you to create different levels of security by restricting or allowing network activity with a rule that is enforced based on traffic's origination or destination Zone.

This section contains the following topics:
- “Introduction to Zones,” in the following section
- “Introduction to Zone Rules,” on page 58

Introduction to Zones

Zones are virtual spaces—ways of classifying the computers and networks with which a protected computer communicates.

**Trusted Zone**

The Trusted Zone contains traffic sources that you know and trust. In designing policies, you configure the Trusted Zone to include only the network elements your protected computers need to communicate with. Do not place your entire network in the Trusted Zone.

Consider the following when configuring your Trusted Zone:
- Remote host computers connected to the protected computer (if not included in the subnet definitions for the corporate network)
- Corporate Wide Area Network (WAN) subnets that will be accessed by the protected computer
- Corporate LANs that will be accessed by the protected computer
- Check Point Endpoint Security Server
- DNS servers
- Local host computer's NIC loopback address (depending on Windows version). If you specify a local host loopback address of 127.0.0.1, do not run proxy software on the local host.
- Internet gateways
- Local subnets
- Security servers (for example, RADIUS, ACE, or TACACS servers)

**Blocked Zone**

The Blocked Zone contains traffic sources that you don’t want your protect computers communicating with at all. In designing policies, you will populate the Blocked Zone with dangerous or otherwise undesirable hosts. You may choose to include dangerous,
or undesirable external locations, or internal locations that you want to restrict access to, such as Human Resources servers.

**Internet Zone**

The Internet Zone contains all traffic sources that you have not placed in either the Trusted Zone or Blocked Zone. Internet Zone sources may be outside or inside the perimeter firewall, anywhere on your local network or on the Internet.

By default, all sources and destinations of network traffic are in the Internet Zone. By placing trusted traffic sources in the Trusted Zone, you can give your endpoint users access to needed resources while keeping them safe from Internet threats.

**Introduction to Zone Rules**

Using Zone rules, the client analyzes traffic to and from the protected computer in terms of the Zone the traffic is coming from or going to, and the ports and protocols involved. If program control is enabled, it also analyzes the traffic in terms of the application on the protected endpoint computer that is sending or receiving the traffic.

For information about how Zone Rules interact with other security settings, see “Rule Evaluation and Precedence,” on page 43.

The following settings are provided:

- **Low** security essentially removes endpoint protection except for Program Control. This level is recommended only for environments where threats or intrusions are known to be absent.

- **Medium** security allows most commonly used network protocols. This level is recommended for the Trusted Zone in security policies for protected computers on a Local Area Network (LAN). Medium security also enforces Program Control.

- **High** security establishes the strongest level of security by restricting most traffic types. This level is recommended for the Internet Zone of protected computers connected directly to the Internet or connected via an insecure network (such as a remote user's ISP).

You can also customize your security level to meet your needs.
Workflow for Zone-Based Security

The process for setting up and using Zone-based security consists of the following steps:

1. Configure new network detection options.
   This setting controls what the client does when it encounters an unfamiliar network. See "Configuring New Network Detection Options," on page 60.

2. Configure the Trusted and Blocked Zones
   a. Research your network setup to see which subnets, hosts, or other resources need to be trusted or blocked.
   b. Create location definitions
   c. Add the locations to the appropriate Zone.
   See “Defining Zones,” on page 60.

3. Configure Zone rule settings.
   Configure Zone rule settings to specify which traffic is allowed for the Trusted and Internet Zones. See “Setting Security Levels,” on page 61.

4. Add new trusted and blocked locations as they are identified.
   Over time, you will identify new computers and networks to either trust or block. Incorporate them into your setup by creating new locations and adding them to the appropriate Zones.
Managing Zone-Based Security

Use the instructions in this section when managing security based on Zones.

Configuring New Network Detection Options

New network detection options determine what the client does when the protected computer connects to a network that has not already been placed in the Trusted Zone or Internet Zone. Use the Endpoint Security Administrator Console to configure your network detection options.

To set up a security policy's access Zones:

1. Go to the Access Zones page.
   For navigation information, see “Access Zones,” on page 190.
2. Select the option you want for When a new network is detected by the client.
   For more information about completing these options, see the Endpoint Security online help.
3. Click Save.
   For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

Defining Zones

Define your Zones by adding the appropriate locations to them. You can create locations as you need them from the Zones tab, or you can create your locations in the Location Manager and then add them to the Zones.

To configure Zones:

1. Go to the Access Zones page.
   For navigation information, see “Access Zones,” on page 190.
2. In the Define Zones area, click Add.
3. Select the locations and choose the Zone to put them in.
4. Click Add.
5. Click Save.
   For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

If endpoint users experience network access problems after a policy deployment, check your Trusted Zone contents first to make sure no needed elements are missing.
Setting Security Levels

To ease administration, Endpoint Security provides three pre-configured security levels that you can apply immediately to the Internet Zone or Trusted Zone. Use the Endpoint Security Administrator Console to set the security levels for your Zones.

To configure Security Rules:
1. Go to the Access Zones page.
   For navigation information, see “Access Zones,” on page 190.
2. In the Security Rules for Internet and Trusted Zones area, choose the security settings you want.
   You can use the preconfigured settings, or click the Show Settings button to create custom settings for the Medium or High security settings.
   If you have changed the settings from the default values and need to view the default settings, view the original version of the default policy. See “Managing Policy Versions,” on page 54.
3. Click Save.
   For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

Configuring Advanced Packet Handling Settings

Advanced packet handling settings apply to all traffic, regardless of Zone. These rules enable you to defend against packet fragment attacks, and block or allow VPN protocols or uncommon protocols when High security is being applied.

To configure advanced settings:
1. Go to the Access Zones page.
   For navigation information, see “Access Zones,” on page 190.
2. In Security Rules for the policy, select the packet types and conditions you want to block.
   For more information about these options, see the Endpoint Security online help.
3. Click Save.
   For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.
In This Chapter

Introduction to Firewall Rules  page 63
Firewall Rule Workflow  page 65
Managing Firewall Rules  page 66

Implementing firewall rules achieves the same level of security as standard perimeter firewalls by restricting or allowing network activity based on connection information, such as IP addresses, ports, and protocols, regardless of the program sending or receiving the packet.

Use firewall rules to:

- Create a standard perimeter firewall on the protected computer. See “Firewall Rule Workflow,” on page 65.
- Fine-tune program control by restricting the network access of a program or program group. See “Program Control,” on page 69.
- Restrict the access of users that are not compliant with your security policies. See “Adding Restriction Firewall Rules to Your Policy,” on page 117.
Introduction to Firewall Rules

Firewall rules (referred to as “expert rules” in the Flex client user interface and user manual) block or allow network traffic to or from the endpoint computer based on attributes of communication packets. You can use firewall rules to block or allow traffic based on the following three attributes:

- Source or destination locations
- Protocol and/or port
- Time activities occurs

There are two types of firewall rule:

- Incoming - controls network traffic coming to the endpoint computer.
- Outgoing - controls network traffic coming from the endpoint computer.

Firewall Rule Rank in Security Policies

In a security policy, rank is the order in which a client evaluates and executes the firewall rules. Because clients execute the first rule that matches the traffic, the rule’s rank is extremely important.

Example of FTP Access

The example in this section uses the following two FTP access rules to demonstrate how rank affects network activity.

- The rule FTP Local allows FTP clients from the local private subnet (Private Subnet) to connect to the protected computer’s FTP server on port 21.
- The rule FTP Internet blocks all FTP clients from connecting to the protected computer’s FTP server on port 21.

Example 1: Allow local traffic and block other traffic

In the first example, FTP Local is rank 0 and FTP Internet is rank 1.

- FTP requests from clients on the local subnet match the source address (Private Subnet) and all other conditions of the FTP Local rule. The client executes FTP Local; the traffic is allowed.
- FTP requests from clients outside the local subnet do not match FTP Local conditions, so the client checks the next rule (FTP Local is not executed). The traffic matches the conditions of FTP Internet. The client executes FTP Internet; the traffic is blocked.

Figure 8-1: Example with FTP Local rule rank 1
Example 2: All access is Blocked

Figure 8-2: Example with FTP Internet rule rank 1

<table>
<thead>
<tr>
<th>Rank</th>
<th>Notes</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Time</th>
<th>Action</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>FTP Internet</td>
<td>Any</td>
<td>Any</td>
<td>FTP</td>
<td>Always</td>
<td>Block</td>
<td>None</td>
</tr>
<tr>
<td>1</td>
<td>FTP Local</td>
<td>Private Subnet</td>
<td>Any</td>
<td>FTP</td>
<td>Always</td>
<td>Allow</td>
<td>Log</td>
</tr>
</tbody>
</table>

In the second example, FTP Internet is rank 0 and FTP Local is rank 1.

- All FTP requests from clients on the local subnet and other all locations match the conditions of the first rule, FTP Internet. The client executes FTP Internet; all traffic is blocked.

When FTP Internet is rank 1, traffic always matches the conditions of the first rule. Therefore, the client will never evaluate traffic against second rule, FTP Local.
Firewall Rule Workflow

Use this workflow to create firewall rules and use them in your security policies.

1. Create firewall rules.
   - You can create your firewall rules before creating your policy, using the firewall rules manager, or you can create them as you need them from within the policy.
   - See “Creating Firewall Rules,” on page 66.

2. Add your firewall rule to your policy.
   - See “Adding Firewall Rules to Policies,” on page 66.

3. Rank your firewall rules.
   - Rank your firewall rules to determine which rule takes precedence.
   - See “Ranking Firewall Rules,” on page 67.

4. Deploy your policy.
   - You must deploy your policy for your changes to take effect. See “Deploying Policies,” on page 49.
Managing Firewall Rules

This section explains how to use the Firewall Rule Manager to create, edit, and delete firewall rules.

This section contains the following topics:

- “Creating Firewall Rules,” on page 66
- “Adding Firewall Rules to Policies,” on page 66
- “Ranking Firewall Rules,” on page 67
- “Editing Firewall Rules,” on page 68
- “Deleting a Firewall Rule,” on page 68

Creating Firewall Rules

Create your firewall rules for your ports and destinations. You can define your ports and destinations before creating your firewall rules using the Ports and Protocols manager and the Locations manager. Or you can define them as you need them while creating your firewall rules. Use the Endpoint Security Administrator Console to create firewall rules.

To create a firewall rule:

1. Go to the Firewall Rule Manager page.
   For navigation information, see “Firewall Rule Manager,” on page 192.
2. Click New Rule and choose the type of rule.
3. Complete the information for the rule.
   For more information about completing the rule information, see the Endpoint Security online help.
4. Choose locations and ports for the rule.
5. Click Save.
   For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

Adding Firewall Rules to Policies

Add your Firewall Rule to a security policy. The same Firewall Rule can be assigned to different security policies.

To add a firewall rule to a policy:

1. Go to the Firewall Settings page.
   For navigation information, see “Firewall Settings,” on page 192.
2. **Click Add.**
   
   Rules that are already in the policy are not listed.

3. **Select the rule, and click Add.**
   
   The rule is automatically ranked and enabled.

4. **Click Save.**
   
   Endpoint users will not receive the new policy until you deploy it. For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

---

**If you have a rule that blocks or allows all traffic, do not enable logging for Firewall rules.**

### Ranking Firewall Rules

The Firewall Settings tab contains a list of all the firewall rules in a policy. These rules are listed in order of evaluation and execution priority (rank). The client executes only the first firewall rule to match the traffic.

Before ranking rules, see “Firewall Rule Rank in Security Policies,” on page 63, for examples of how rank determines the behavior of the client.

**To rank a firewall rule:**

1. Go to the **Firewall Settings** page.
   
   For navigation information, see “Firewall Settings,” on page 192.

2. Use the arrow buttons to rank the firewall rules.

3. **Click Save.**
   
   Endpoint users will not receive the new policy until you deploy it. For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

### Enabling and Disabling Firewall Rules

After adding a rule to a policy, you can temporarily disable it without removing it from the policy. Disabled rules don’t affect network traffic and have no rank. Enabled rules are evaluated and executed in the rank order, and affect network traffic.

**To enable and disable rules:**

1. Go to the **Firewall Settings** page.
   
   For navigation information, see “Firewall Settings,” on page 192.
2. To enable or disable the rule, select a rule:
   - Click **Disable**
     The rule's rank is changed to Disabled.
   - Click **Enabled**.
     The rule's rank appears.
3. Click **Save**.

Endpoint users will not receive the new policy until you deploy it. For more information about saving and deploying your policy, see "Creating Policies," on page 49 and "Deploying Policies," on page 49.

**Editing Firewall Rules**

When you modify a firewall rule, the rule settings are automatically updated in all your security policies. However, the policies must be re-deployed before the changes affect the endpoint users.

**Removing Firewall Rules from a Policy**

Removing the rule from a policy does not delete it from Endpoint Security. The rule is still available in the Firewall Rule Manager, and can be added to a policy at any time.

The remaining rules in the policy ranks are renumbered sequentially, preserving their relative ranks.

**Deleting a Firewall Rule**

Deleting a firewall rule automatically removes it from all security policies. However, the policies must be re-deployed before the changes affect the endpoint users.
Chapter 91

Program Control

In This Chapter

Introduction to Program Control  page 70
Program Control Workflow  page 74
Managing Program Control  page 80

Program rules restrict network access on a per-program basis.
Whereas Firewall Rules restrict access according to package content, and Zone Rules according to location, Program Control allows you to restrict network access between a particular program and either your Trusted or Internet Zone. This restriction is at the program level.

Because program rules only restrict access through restricting the application on the endpoint computer, they cannot block access to the endpoint computer using that application from another location. For example, adding a firewall rule to block ICMP packets in the program rule for ping.exe does not prevent the endpoint computer from being pinged or 'hide' it from others. This is because incoming packets are handled by a system process, not by ping.exe. To 'hide' an endpoint computer, use the firewall rules in the Firewall tab.

Program Control only moderates network access for programs. It does not prohibit the programs themselves. To require or prohibit a program on an endpoint computer use enforcement rules. See "Introduction to Enforcement Rules," on page 98.

Check Point’s Program Advisor service streamlines program management by providing professionally-recommended security settings for most programs. If you are using Program Advisor, you will be able to skip most of the topics in this chapter. See "Program Advisor," on page 87 for information about managing programs and program permissions using Program Advisor.
Introduction to Program Control

Use Program Control to moderate the access your programs have to the Trusted or Internet Zone. Program Control uses program permissions applied to individual programs or program groups to control program activity.

This section contains the following topics:
- “Program Permissions,” on page 70
- “Program Groups,” on page 71
  - “Default Groups,” on page 71
  - “Custom Groups,” on page 71
- “Permission Precedence,” on page 72
- “Global and Policy Permissions,” on page 72
- “Program Evaluation Process,” on page 72
- “Using Checksums,” on page 73

Program Permissions

Program permissions control the programs on endpoint computers. You can set the permissions for individual programs or groups of programs. Program activity is evaluated according to the following criteria:

- Zone - Traffic is evaluated by the Zone (Internet or Trusted) that the program is trying to communicate with.
- Role - Traffic is evaluated according to whether the program is trying to establish a connection (acting as a client) or listen for a connection (acting as a server)?

You can set the following permissions for programs and program groups:

- Allow - Allows the program to establish or accept the connection
- Block - Blocks the program from establishing or accepting the connection
- Ask - Asks the endpoint user whether to allow or block the program
- Terminate - Denies the connection and terminates the program.

If you choose the ‘Ask’ permission, you must also choose the Allow Flex clients to decide ‘Ask’ program permissions option in the Advanced Client Settings on the Program Rules page. If you do not, Flex will not ask the user for program permissions.
Program Groups

Your endpoint users may use hundreds, or even thousands of programs. To facilitate managing your programs, it is recommended that you generally set program permissions for groups of programs, rather than for individual programs. Check Point provides some program groups. You can also create custom groups to manage your programs.

Groups exist only on the Endpoint Security server. Endpoint users with Flex see only the individual program permissions whether individually assigned or inherited from a group.

Default Groups

Check Point provides the following default program groups:

- **PA quarantined programs** - If you are using Program Advisor, this group contains all the programs that Program Advisor recommends terminating. This group has precedence over all other groups. You cannot change the rank of this group, disable this group, or override its group permissions. You can, however, override the permissions for the individual programs in this group, but this is not recommended. If you do not have a Program Advisor license, this group does not appear.

- **PA referenced programs** - If you are using Program Advisor, this group contains all the programs that Program Advisor recommends allowing or asking the user about. This group always ranks immediately after your custom groups. You cannot change the rank of this group or override its group permissions. You can, however, disable this group or override the permissions for the individual programs in the group. If you do not have a Program Advisor license, this group does not appear.

- **Unrecognized programs** - This group contains all the programs that are not governed by any other group. Programs remain in this group until you create groups for them. This is always the lowest-ranking group. You cannot change the rank of this group.

Custom Groups

You can also create custom groups. Custom groups act as filters, grouping programs 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 the same program. This is useful when your users are using many different versions of the same program, such as Microsoft Outlook. You can also use this for programs that change checksum frequently, such as programs that your organization is creating.
Permission Precedence

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

- PA quarantined programs
- Custom groups, in the order they appear in the Program Group Permissions page.
- PA referenced programs
- Unrecognized programs

You can change the order of your custom groups, but you cannot change the order of any of the default groups.

If you need to make an exception to the permissions for a group, you can set individual permissions for that program. Generally, for maximum efficiency you should set permissions on the group level whenever possible and only make exceptions when absolutely necessary.

Global and Policy Permissions

You can set permissions for programs either at the global level or in individual policies. Global program permissions are set in the Program Group Permissions page and apply to your entire organization.

Policy-level program permissions are set in the policy. They only apply to the endpoint computers that receive that policy.

It is recommended that you configure your global program permissions to reflect your general security needs and then use policy-level permissions to create any special exceptions.

Although you can configure program permissions at both the global and the policy level, both settings are included in your security policy. You must redeploy your policy to have either global or policy-level changes take effect.

Program Evaluation Process

In case of conflict between policy-level and global permissions, they are enforced in the following order:

1. Policy-level permissions for a particular program
2. Global permissions for a particular program
3. Policy-level permissions for the program group
4. Global permissions for the program group

The permission setting for the program is always displayed in the policy, in the program permission pages. Policy-level permissions are shown in color. Global permissions are shown in gray.
Using Checksums

You may wish to identify programs by their checksums, instead of by filename alone. 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 that your endpoint computers have. 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 your endpoint 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.
Program Control Workflow

Although many of the program control tasks can be performed at any time, it is recommended that you begin by performing the steps in this workflow. This workflow assumes that you have already configured your Zones. See “Zone-Based Security,” on page 56.

To configure program control:
1. Gather programs.
   Populate program control with the programs that are running on your endpoint computers. You can use any or all of the following detection methods:
   • Appscans. See “Creating Appscans,” on page 80.
2. Plan your permission settings.
   Plan your policy lifecycle to balance security with user access. See “Planning Program Control,” on page 75.
3. Create your global program groups and assign permissions.
   Program groups act as filters, applying the same permissions to programs that meet their parameters. See “Creating Program Groups,” on page 84.
4. Configure any exceptions to your global program group permissions.
   Global program group permissions apply to all the programs in that group, unless you override the group permissions with permissions you configure for the individual programs. See “Setting Program Permissions,” on page 84.
5. Set your policy-level program permissions.
   The program group permissions you set at the policy level supersede permissions set at the global level. See “Setting Policy-Level Permissions,” on page 85. For more information about how global and policy-level permission interact, see “Program Evaluation Process,” on page 72.
6. Configure your alert levels.
   If you have program permissions that are configured to ask the endpoint user, you will need to allow program alerts. If you do not use permissions that ask the endpoint user, you may want to configure your alert levels to minimize the alerts the endpoint users see. See “Configuring Alert Levels,” on page 86.
7. Monitor your programs.
   Periodically check for new programs that are not handled by your program groups or Program Advisor. Use the Search function to find programs that were first observed within the last week or last 24 hours. You can then create program groups to handle these programs.
Planning Program Control

As with most security settings, your program control permissions must balance user access with security. You should pay particular attention to the settings you apply to Unknown Programs.

This section contains the following topics:

- “Program Permission Considerations,” on page 75
- “Configurations for Unknown Programs,” on page 76

Program Permission Considerations

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.

Generally, it is recommended that you begin your implementation with a permissive policy, that uses lenient program permissions and then later tighten your security with progressively more restrictive policies. This iterative policy creation process is known as a ‘policy lifecycle’. For more information about policy lifecycles, see the Endpoint Security Implementation Guide.

Table 9-1 lists the behaviors from the most to the least risk.

Table 9-1: Program behaviors in order of risk

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Zone/Act as Server</td>
<td>Allows the application to listen for a connection from a non-trusted server.</td>
</tr>
<tr>
<td>Internet Zone/Act as Client</td>
<td>Allows the application to connect to non-trusted computers.</td>
</tr>
<tr>
<td>Trusted Zone/Act as Server</td>
<td>Allows the application to listen for a connection from a trusted server.</td>
</tr>
<tr>
<td>Trusted Zone/Act as Client</td>
<td>Allows the application to connect to servers in the Trusted Zone.</td>
</tr>
</tbody>
</table>

Internet Zone/Act as a Server

In most cases, you should not allow programs to act as servers to the Internet Zone. There are few reasons a standard workstation needs to accept connections.

Generally, you should prevent this kind of network activity for Unknown Programs, because this type of connection presents the greatest risk. Remote access Trojan horse programs can listen for connections from hackers and unauthorized, unpatched FTP and Web servers can be exploited to gain access to your network.
Internet Zone/Act as a Client
To protect your network from common threats such as key loggers or remote access Trojan horse programs, you should generally not allow programs to act as clients to computers in the Internet Zone.

However, there are legitimate reasons for some programs to have this kind of network access. For example, applications with auto-update functions, mail clients, instant messengers, and Web browsers all need to be able to access the Internet to perform their functions. To unblock legitimate applications, you must either add the locations that the applications need to access to the Trusted Zone, or allow the application to act as a client in the Internet Zone.

Trusted Zone/Act as a Server
You may want to prevent this kind of access for some programs to help prevent against attacks launched from inside your organization. You may also want to prevent this kind of access on certain computers that contain highly sensitive data. However, some programs legitimately need Trusted Zone server access for features such as drive sharing. Also, some endpoint users may have a legitimate need to run server programs on their endpoint computers.

Trusted Zone/Act as a Client
This is generally the least risky type of communication to allow. Generally, you will want to allow applications to have this kind of access to allow access to printers, remote files, and internal Website locations. Generally, you will only want to broadly restrict this kind of access as a temporary measure in response to a serious attack.

Configurations for Unknown Programs
Since unknown programs generally present the most risk to your network, you should pay particular attention to the permissions you assign to them. However, setting excessively restrictive permissions too early in your implementation may lead to blocking legitimate traffic. This can be very disruptive to your endpoint users.

For these reasons, it is generally recommended that your first policies use less program permissions. Once you have populated the system with the more commonly used programs and sorted them into groups, you can gradually apply stricter program permissions.

Sample Program Permission Configurations
Use these sample program permissions for unknown programs when managing program control. The sample permissions are presented in order from most lenient to most restrictive. Generally, this is the order in which you should implement them in your security policies. Each sample 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?
- **Policy maintenance** - How much time will you have to spend maintaining the policy by adding exceptions and specific program permissions?

As a general rule, the more restrictive you are with these settings, the more protection you have from unknown attacks, but the more work you will have to put into maintaining the policy.

**Table 9-2:** Sample Permission for Unknown Programs

<table>
<thead>
<tr>
<th>Sample</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>Block Internet Zone servers only</td>
<td>Allow</td>
</tr>
<tr>
<td>Block all servers</td>
<td>Block</td>
</tr>
<tr>
<td>Block All non-trusted communication</td>
<td>Allow</td>
</tr>
<tr>
<td>Block All</td>
<td>Block</td>
</tr>
</tbody>
</table>

**Block Internet Zone servers only**

This is the most lenient of the sample settings for Unknown Programs. Because applications accepting connections from the Internet pose the greatest risk to the endpoint, this configuration provides effective security by blocking those connections.

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

**Table 9-3:**

<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 any program that sends traffic to the network. They are also able to run any programs that accepts a connection from a trusted host.</td>
</tr>
<tr>
<td>Policy 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>

**Block all servers**

Use these settings for your Unknown Programs if you don't want to assume the Trusted Zone is safe to accept connections from. 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.
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 within your network.

Table 9-4:

<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>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 any program that send traffic to the network. They are not able to run any programs that accept connections.</td>
</tr>
<tr>
<td>Policy 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>

Block All

The block all option completely 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 your endpoint users.
Table 9-6:

<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>Any application trying to send traffic or accept a connection from the Internet Zone is blocked.</td>
</tr>
<tr>
<td>User restriction</td>
<td>High</td>
<td>Users are able to run any program that communicates within the Trusted Zone. If a program communicates anywhere on the Internet Zone, it is blocked.</td>
</tr>
<tr>
<td>Policy maintenance</td>
<td>High</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>
Managing Program Control

Use the Endpoint Security Administrator Console to manage program control.

This section contains the following topics:

- “Creating Appscans,” on page 80
- “Adding Programs Manually,” on page 83
- “Creating Program Groups,” on page 84
- “Setting Program Permissions,” on page 84
- “Setting Policy-Level Permissions,” on page 85
- “Configuring Alert Levels,” on page 86

Creating Appscans

A 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.

Create an Appscan for each disk image used in your environment. You can then create rules that will apply to those applications. Using Appscans to populate your Endpoint Security system is particularly useful if your endpoint computers tend to have the same programs.

You create Appscans by running the SmartSum utility (appscan.exe) on a computer with a tightly-controlled disk image, then importing the file into Endpoint Security.

Follow these steps to use Appscans:

1. “Creating an Appscan,” on page 80
2. “Importing Appscans,” on page 83

Creating an Appscan

Before running Smart checksum, set up a computer with all the programs that are standard for protected computers in your organization. If you have several different configurations, perform these steps for each endpoint computer standard configuration.

The computer you scan to create a Appscan must be free of all malware. If you are certain that your scan is “clean,” you can create rules that allow the programs access to the network.

To run SmartSum from the command line:

1. Copy SmartSum, located in the \CheckPoint\Integrity\engine\webapps\ROOT\bin directory on the
Endpoint Security host, to the root directory (typically c:\) of the baseline reference source computer.

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

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

2. On the protected computer, open a command prompt window (go to Start | Run..., then type cmd).

3. In the command prompt window, go to the root directory by entering "cd \".

To limit the scan to a specific directory, go to that directory, then begin your scan there (for example, cd 'program files').

4. Type appscan \ to begin the scan.

You can modify the scan through the use of the Appscan switches. See “Appscan Switches,” on page 81.

When the scan is complete, an output file (scan.xml) is created in the directory where you ran the scan and the command prompt appears.

Your Appscan file is ready to be imported into Endpoint Security. See “Importing Appscans,” on page 83.

**Appscan Switches**

Use the following switches to modify your scan.

**Table 9-7: Appscan switches and functions**

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/o</td>
<td>Specifies the output file to be created. If no file name is specified, the default output file name (scan.xml) is used.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> C:\appscan /o scan1.xml [files]</td>
</tr>
<tr>
<td></td>
<td>In Example 1, the scan is named scan1.</td>
</tr>
<tr>
<td></td>
<td>• The output file name is important since you will be using this file when importing it into the Endpoint Security server.</td>
</tr>
<tr>
<td></td>
<td>• If you conduct multiple scans on the same machine, give each scan a unique name.</td>
</tr>
</tbody>
</table>
Table 9-7: Appscan switches and functions

<table>
<thead>
<tr>
<th>Switch (Continued)</th>
<th>Function</th>
</tr>
</thead>
</table>
| /x | Designates the target file names to add to the scan.  
- The leading period before a file extension is required.  
- A semi-colon separates the target extensions.  
- The target extensions are grouped by quotes.  
- A target directory must be specified using the /s switch.  
- If the /x switch is not used in the command statement: Only program files (.exe file name extension) are scanned.  
Example 2: C:\appscan /o scan2.xml /x "*.exe;.dll" /s "C:\"  
In Example 2, the scan is named scan2, and the scan will include .exe and .dll files in the current directory only. |
| /s | Designates the directory for SmartSum to inventory.  
- If you do not use /s to designate a target directory, the scan will be run in the current directory only.  
- If you use /s, the scan will be run in the target directory and its subdirectories.  
Example 3: C:\appscan /o scan3.xml /x "*.dll" /s C:\program files  
In Example 3, the scan is named scan3. The target directory is C:\program files and all its subdirectories. The target extension is .dll.  
Example 4: C:\appscan /o scan4.xml /x "*.exe;.dll" /s C:\program files  
In Example 4, the scan is named scan4. The target directory is C:\program files. The target extensions are .exe and .dll. |
| /e | Use the /e switch to inventory all executable files in the target directory or drive, regardless of extension.  
Example 5: C:\appscan /s "C:\program files" /e  
In Example 5, all files are incorporated into the scan. |
| /a | Generates all file properties for each file inventoried.  
Example 6: C:\appscan /o scan6.xml /s "C:\" /a  
In Example 6, the scan is named scan6. The target directory is the entire contents of c: The output file displays file properties more thoroughly than it would without the /s switch.  
The /s switch does not affect the source. |
| /p | Displays progress messages. |
| Iverbose | Displays progress and error messages. |
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.

To import an Appscan:

1. Go to the Program Group Permissions page.
   For navigation information, see “Program Group Permissions,” on page 193.
2. Click Add Programs and select Import Scan.
3. Specify the Appscan file by browsing to it:
   a. Click Browse.
   b. Locate the scan.xml.
   c. Click Open.
4. Click Import.

You must remove all special characters, such as trademarks from the appscan before importing it.

Adding Programs Manually

If there is a program that has not been observed on your system that you want to proactively set permissions for, you can add it manually. Adding programs manually and then setting the global program permissions to ‘block’ is especially useful for protecting your system from new malicious programs.

To manually add a program:

1. Go to the Program Group Permissions page.
   For navigation information, see “Program Group Permissions,” on page 193.

---

Table 9-7: Appscan switches and functions

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Displays warning messages.</td>
</tr>
<tr>
<td>-</td>
<td>Displays help for SmartSum.</td>
</tr>
</tbody>
</table>

You must remove all special characters, such as trademarks from the appscan before importing it.
2. Click Add Programs and select Add Manually.
3. Enter the information for the program and click Save.

For more information about completing the program information, see the Endpoint Security Online Help.

Creating Program Groups

Endpoint Security comes with some default program groups. You should create additional, custom program groups to facilitate managing your program permissions. Program groups allow you to assign permissions to entire groups of programs at once.

Program groups act as filters, grouping programs according to the criteria you specify. As programs are added to the Endpoint Security system, they are automatically added to the appropriate group and the permissions you specify for that group are enforced.

To create a custom program group:

1. Go to the Program Group Permissions page.
   For navigation information, see “Program Group Permissions,” on page 193.
2. Click New Group.
3. Configure the information for this program group.
   You can use either standard Windows wild cards, such as ‘*’ or ‘?’ or Java regular expressions to specify your filter information. Java regular expressions must be preceded by a ‘|’. For more information about configuring the program group information, see the Endpoint Security Online Help.
   a. Enter the Group Definition information.
   b. Enter the Filter Settings.
      These settings determine which programs will be added to this group.
   c. Configure the Permission Settings for the group.
      These settings determine the network access for the programs in the group.
4. Click Save.
5. Redeploy your policies.

Although you can configure program permissions at both the global and the policy level, both settings are included in your security policy. You must redeploy your policy to have either global or policy-level changes take effect.

Setting Program Permissions

You can set program permissions for groups of programs. See “Creating Program Groups,” on page 84. This is the recommended way to set permissions for most programs.
You can also set permissions for individual programs. These permissions override the permissions set for the program group. Permissions given to an individual program persist even if the program changes groups.

**To set individual program permissions:**

1. Go to the **Program Group Permissions** page.

   For navigation information, see “Program Group Permissions,” on page 193.

2. Click the **Group Name** of the group that the program belongs to.

3. Click the **Program Name**.

4. In the **Permissions Settings** area, configure the permissions.

   For more information about configuring the permission options, see the Endpoint Security Online Help.

5. Click **Save**.

---

**Setting Policy-Level Permissions**

Use policy-level permissions to set exceptions to your global rules for the endpoint computers that receive that policy.

**To set policy-level permissions**

1. Go to the **Program Group Permissions** page of the policy.

   For navigation information, see “Program Group Permissions,” on page 193.

2. Change the permissions for the group or an individual program.

   - To change the permissions for a group, click **Override** in the row for that group and perform the following steps:
     a. Set the permissions for the group.
     b. Click **Save**.

   - To change the permissions for an individual program, click the name of the group that the program belongs to and perform the following steps:
     a. Click **Override** in the row for the program.
     b. Set the permissions for the program.
     c. Click **Save**.

3. Set firewall rules (optional)

   You can also choose to add firewall rules to your program rule settings. Use firewall rules to restrict access to certain areas within the allowed Zones.

   a. In the rules page for a group or program click **Add** in the Firewall Rules section.
b. Choose the firewall rules and click Add.
   If needed, you can create new rules using the New Firewall Rule button.

c. Click Done.

Firewall rules are enforced in the order listed. These rules are applied only if
the program has the required permission to act as a server or act as a client
for the Zone involved.

4. Click Save.

Configuring Alert Levels

The Endpoint Security clients can alert endpoint users whenever programs try to
perform restricted functions. To avoid overwhelming endpoint users with alerts, you
may want to prevent the clients from showing all of these alerts.

To configure alert levels:

1. Go to the Client Settings page.
   For navigation information, see “Client Settings,” on page 191.

2. In the Client Alerts and Logs area, configure the Program Alerts according to your
   needs.
   For more information about configuring alerts, see the Endpoint Security Online
   Help.

3. You can also optionally prevent alerts for particular groups or programs by using
   the Suppress Alerts feature in the permissions page for a program or program
group.

4. Click Save.
   For more information about saving and deploying your policy, see “Creating
Chapter 10
Program Advisor

In This Chapter

- Introduction to the Program Advisor Server page 88
- Introduction to the Program Advisor Process page 89
- Program Advisor Workflow page 93
- Managing Program Advisor page 94

Smart Defense Program Advisor is a service provided by Check Point that gives policy recommendations for programs. 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 lets you choose to terminate malicious programs on endpoint computers.
Introduction to the Program Advisor Server

The Program Advisor Server contains a database of program permissions that is constantly updated by Check Point security professionals. The Program Advisor Server can perform the following functions:

- Provide program permissions to the Endpoint Security server
  You can choose to either accept these permission recommendations or override them with custom recommendations of your own.

- Provide program permissions to the client
  You can configure the enterprise policy to allow the client to access the Program Advisor Server directly if the client cannot contact the Endpoint Security server.
Introduction to the Program Advisor Process

The Program Advisor process begins when a program on an endpoint either accesses the Internet, or is accessed by the Internet.

Client Program Advisor Process Diagram

Figure 10-1: Client Process

The following steps describe the client Program Advisor process:

1. The program starts and the client checks for locally-stored permissions for the program.

   The client has two sets of locally-stored permissions: those set by the endpoint user, and those set by the enterprise policy.
   - If the client finds locally-stored permissions for the program, it checks the time-to-live date.
If the client does not find locally-stored permissions, it will attempt to contact the Endpoint Security server to check permission settings.

2. The client checks the program permission time-to-live date.
   If the client finds locally-stored permissions, and the policy is set to allow the client to ask the Endpoint Security server, it checks the time-to-live.
   • If the time-to-live has not expired, the client uses the locally-stored permissions.
   • If the time-to-live has expired, the client will attempt to contact the Endpoint Security server to check for new permission settings.

3. The client asks the Endpoint Security server.
   If the client does not find locally-stored permissions, or the permission time-to-live has expired, the client attempts to contact the Endpoint Security server to obtain program permissions. See the “Endpoint Security Program Advisor Process Diagram,” on page 91 for more information about this process.

   In the case of Flex users with policy arbitration enabled, Flex will both ask the user whether or not to allow access and attempt to contact the Endpoint Security server for program permissions. Flex records the results of both queries in the personal and enterprise policies, respectively.

4. The client asks Program Advisor server.
   If the client does not find locally-stored permissions, or the permission time-to-live has expired, and the client is not able to contact the Endpoint Security server, and you have set the policy to allow the client to ask the Program Advisor server, it attempts to contact the Program Advisor directly to obtain program permissions. In Simple view, the client always has permission to ask the Program Advisor server.

5. The client performs client-specific actions.
   • If your endpoints are using Flex and you have set the policy to not allow the client access to the Endpoint Security server or to not allow access to the Program Advisor Server, the client will ask the user whether or not to allow access.
   • If your endpoints are using Agent and you have set the policy to not allow the client access to the Endpoint Security server or to not allow access to the Program Advisor Server, the client will block access to and from the program.
The Endpoint Security server receives program permission requests from the client. In conjunction with the Program Advisor server, it determines what permissions should be applied to the program, and how it should be displayed in the Program Group Permissions page of the Endpoint Security Administrator Console.

1. The Endpoint Security server receives the request from the client.
2. The Endpoint Security server checks for a matching reference source.
   If the program has a matching reference source, the Endpoint Security server
   sends a response to the client. The client applies the permissions you have set for
   referenced programs in the deployed enterprise policy.

3. The Endpoint Security server checks if Program Advisor is enabled.
   If Program Advisor is not enabled, the Endpoint Security server sends a response to
   the client. The client applies the permissions you have set for ‘Unknown Programs’
   in the deployed enterprise policy.

4. The Endpoint Security server checks for custom overrides.
   You can set the Endpoint Security server to override Program Advisor’s
   recommendations with your own, custom permission set. If you have set custom
   overrides for this program, the Endpoint Security server sends a response to the
   client. The client applies the custom permissions you specified.

5. The Endpoint Security server checks for Program Advisor recommendations.
   The Endpoint Security server either contacts the Program Advisor server, or
   accesses a cached copy of the Program Advisor’s previous recommendations.
   Program advisor recommendations stored on the Endpoint Security server include
   a time-to-live stamp. If the time-to-live period has expired for the program, the
   Endpoint Security server must contact the Program Advisor Server to check for new
   permissions.
   • If Program Advisor has a recommendation for this program, the Endpoint
     Security server sends the recommended permissions to the client. The client
     applies the Program Advisor permissions.
   • If Program Advisor does not have a recommendation for this program, the
     Endpoint Security server sends a response to the client, instructing it to mark
     the program as ‘Unknown’ in the Program Group Permissions page. The client
     applies the permissions you have set for ‘Unknown Programs’.
Program Advisor Workflow

Perform the following steps to use Program Advisor effectively.

Implementing Program Advisor:

1. Enable Program Advisor.
   See “Enabling Program Advisor,” on page 94.

2. Configure Endpoint Security to work with a proxy server.
   If you plan to use Program Advisor in an environment that includes a proxy server for Internet access, perform the configuration steps for using proxy login. See “Proxy Configuration,” on page 184.

3. View Program Advisor recommendations.
   See “Viewing Program Advisor Recommendations,” on page 94.

4. Implement any overrides (optional).
   See “Overriding Program Advisor Recommendations,” on page 95.

5. Manage unknown programs.
   See “Managing Unknown Programs,” on page 96.
Managing Program Advisor

This section contains the following topics:
- “Enabling Program Advisor,” on page 94
- “Viewing Program Advisor Recommendations,” on page 94
- “Overriding Program Advisor Recommendations,” on page 95
- “Managing Unknown Programs,” on page 96

Enabling Program Advisor

To use Program Advisor in your policies, you must first license it and configure it. This section explains how to do so.

Use of Program Advisor requires a license. If your license expires, Endpoint Security ceases to respond to program permission requests from clients. Custom overrides also cease to function, including termination. Locally-stored permissions will remain valid until their time-to-live expires.

For Program Advisor to work correctly, the Endpoint Security server must have Internet access so that it can connect to the Program Advisor Server (on ports 80, and 443) and retrieve the latest program information. You must ensure that your firewall allows this traffic. If your environment includes a proxy server for Internet access, perform the configuration steps in “Proxy Configuration,” on page 184, before continuing with the steps in this section.

To enable Program Advisor:

1. Obtain a Program Advisor license key from your Check Point representative or from the Check Point User Center (www.checkpoint.com/usercenter).

2. Use SmartUpdate or the cplic command-line tool to apply the license to the desired installation. For instructions on using SmartUpdate to apply the license, see the SmartCenter User Guide. (You can also use the Check Point Command Line Interface Guide. For information on cplic, see the Check Point Command Line Interface Guide. You can also use the Check Point Configuration Tool to apply licenses locally, though it is recommended to use SmartUpdate instead. For information on the configuration tool, see the Endpoint Security Installation Guide, the Check Point Getting Started Guide, and the configuration tool's associated online help.)

3. Click Save.

Viewing Program Advisor Recommendations

You can view all the program permission recommendations that Program Advisor provides in the Program Group Permissions page.
To view the Program Advisor recommendations:

1. Go to the Program Group Permissions page.
   
   For navigation information, see “Program Group Permissions,” on page 193.

Each program has permissions set for the Trusted Zone and the Internet Zone. For each program, Program Advisor either blocks or allows access, asks the user whether or not to allow access, or terminates the program’s process.

Program Advisor does not display recommendations for programs until they are observed on the endpoint computer. 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.

### Overriding Program Advisor Recommendations

If you find you do not agree with a Program Advisor recommendation for an individual program in the PA referenced programs group, you can override it with your own custom permissions. However, you cannot override the permissions for the Program Advisor Groups, or individual permissions in the PA quarantined programs group. Use the Endpoint Security Administrator Console to override Program Advisor recommendations. You can override permissions at either the global or the policy level.

To override Program Advisor recommendations:

1. Go to the Program Group Permissions or the Program Rules page of the policy, depending on whether you want to change global or policy-level permissions.
   
   For navigation information, see “Program Group Permissions,” on page 193 and “Program Rules,” on page 193.

2. Click PA referenced programs.
   
   A list of all the programs in the group appears. These programs have been observed on your endpoint computers and Program Advisor recommends some kind of access for them.

3. Click the Product Name of the program.

4. Use the Permissions Settings area to select the custom settings you want.
   
   You can override the individual permissions for each Connection Type and Zone with your own settings, or choose to terminate the whole application. For more information about these settings, see the online help.

5. Click Save.
   
   When you set permissions for an individual program, the permissions are displayed in color. Permissions inherited from a group are gray.

   The changes you have made take effect without redeployment.
Managing Unknown Programs

Once you have deployed a policy you should periodically check for unknown programs. Unknown programs are programs that are not referenced, and not governed by either Program Advisor or any other program group. You should set up groups for these programs so you can assign permissions to them more efficiently. Use the Endpoint Security Administrator Console to manage your unknown programs.

To manage unknown programs:

1. Go to the Program Group Permissions page.
   For navigation information, see “Program Group Permissions,” on page 193.
2. Click Unknown Programs.
   View the programs to determine what program groups you need to create.
3. Create program groups as appropriate.
   See “Creating Program Groups,” on page 84 for more information on observing and grouping programs.
In This Chapter

Introduction to Enforcement Rules page 98
Enforcement Rule Workflow page 102
Minimizing Support Requirements page 104
Enabling Enforcement Rule Alerts and Logging page 107
Managing Enforcement Rules page 108
Using Enforcement Rules in a Security Policy page 115
Tracking Enforcement Rule Compliance page 119

Use enforcement rules to ensure that endpoint computers comply with your security policies regarding antivirus and other types of software. If an endpoint computer does not comply with one or more enforcement rules, you can restrict the connection using restriction firewall rules.

Enforcement rules control what programs may be installed on your endpoint computers, not program activity. To control program activity on the endpoint computer, use program rules. (See "Program Control," on page 69 for instructions.)
Introduction to Enforcement Rules

Enforcement rules determine whether the client can establish and maintain a session with the Endpoint Security server and your internal network. The client periodically checks the endpoint computer for the enforcement rule conditions you set.

This section explains:
- “Enforcement Rule Types,” on page 98
- “Enforcement Rules Process,” on page 98
- “What a Restricted User Experiences,” on page 100

Enforcement Rule Types

The Endpoint Security server allows you to create the following types of enforcement rules to secure the endpoint computer:

- **General** — These enforcement rules require or prohibit specific file or program configurations. For example, if you create a rule requiring a specific registry key on Windows NT computers, users establishing a session from a Windows NT computer must have that registry key. Users logging in from Windows NT computers that do not have the registry key are then treated as being out of compliance with the rule. Use these rules to require or prohibit applications that are not controlled by the other rule types. See “General Enforcement Rules,” on page 108.

- **Antivirus** — Antivirus provider rules require a specific antivirus program, version, and configuration on the endpoint. For example, if you configured a rule requiring McAfee VirusScan Version 4.2 or higher, users logging in from computers that do not have this software are then treated as being out of compliance with the rule. See “Antivirus Provider Rules,” on page 109.

- **Client** — Client rules require a client on the endpoint computer. For example, if you create a rule requiring Agent version 7.0, users must have that version of Agent. Users that do not have Agent, or which have the wrong version are then treated as being out of compliance with the rule. See “Client Enforcement Rules,” on page 112.

- **Rule groups** — Rule groups require compliance with a single rule in the group. With a rule group, the computer must be in compliance with at least one of the rules in the group. For example, if you configure a group with rules that require McAfee VirusScan, Symantec Norton AntiVirus, or Trend Micro PC-cillin, then as long as the endpoint computer complies with one of those rules the user is treated as being compliant with the rule. See “Adding and Grouping Enforcement Rules,” on page 115.

Enforcement Rules Process

The client regularly checks the endpoint computer to ensure that it complies with all the enforcement rules in the assigned security policy. If the user's computer becomes out of compliance with the enforcement rule conditions, the client executes the
enforcement action specified by the rule. The following diagram shows the enforcement process.

**Figure 11-1: Enforcement rule process**

1. The client checks the endpoint computer against all enforcement rules in the assigned security policy, including antivirus provider rules and groups. The endpoint computer is found to be either in or out of compliance with the rules.
2. If the endpoint computer complies with all enforcement rules, the client considers it to be ‘in compliance’ and the connection can proceed.
3. If the endpoint computer is in violation of one or more enforcement rules, the client considers it to be “out of compliance.”
4. The client executes the action specified in the enforcement rule. The You can set the client to observe, warn, or restrict computers that are out of compliance. If the enforcement rule is set to ‘Warn’ or ‘Observe’, the action takes place immediately. If the enforcement rule is set to ‘Restrict’ the action takes place after the endpoint computer has been out of compliance for the number of heartbeats you specified.
5. If you have set the enforcement rule to ‘Restrict,’ the endpoint computer will be restricted according to the restriction rules you created for the enforcement rule. The client will set the state to ‘Restricted.’ For more information about restriction
rules and their impact on the user, see “What a Restricted User Experiences,” on page 100.

6. When a endpoint computer is restricted, the client rechecks every minute to see if the computer is back in compliance with the enforcement rules. When the computer is compliant, the client sets the compliance state to ‘In Compliance’ and sends a sync to the server to immediately re-establish full access.

7. If you set the enforcement rule to ‘Observe,’ the computer is allowed to connect and the event is logged. For more information about using the observe feature to minimize support requirements while maintaining security see “Using Rules that Observe or Warn,” on page 105.

8. If you set the enforcement rule to ‘Warn,’ the computer is allowed to connect, the event is logged, and the user sees an alert that describes the security violation and provides a link to remediation information. For more information about how to provide your users with the information they need to resolve their own security violations, see “Providing Remediation Resources for Users,” on page 104.

You can set up remediation resources for endpoints that Endpoint Security has warned or restricted. Warned users must apply the remediation resources manually. Restricted users can apply the resources manually or you can configure Endpoint Security to run the resources automatically.

9. Connected computers are rechecked every heartbeat to ensure that they remain compliant.

There is a delay between the time the endpoint computer becomes non-compliant and the point at which the connection is restricted. The delay is equal to the number of heartbeats you specify before restriction multiplied by the time interval you set for the heartbeats. Observe and warn rules execute on the next heartbeat after non-compliance.

What a Restricted User Experiences

In order to create effective enforcement rules, you should be familiar with the effects your rules have on endpoint users. It is recommended that you attempt to access your network as an endpoint user after you configure an enforcement rule, to be sure that it is having the desired effect and that your endpoints have access to all the resources and information they need to become compliant.

When a endpoint computer is out of compliance with an enforcement rule, the following occurs:

1. The client executes the rule action. The user session is affected as follows:
   - Observed users can access the endpoint network. Observed users receive no alert.
   - Warned users receive an alert, but can still access the endpoint network. If you have configured a remediation resource for the rule, the client includes the resources (for example, a link or an executable file) in the alert message.
Restricted users can access only the part of your network you specify using the restriction rules. If you have configured it to do so, Endpoint Security applies the resource automatically.

Warning and restriction alerts include:

- Default or optional customized text explaining the rule action
- The rule name
- Any additional customized text you defined in the policy (optional)
- A help link that opens the sandbox page you created for that enforcement rule. If you specified a remediation resource, the sandbox page will contain a link to it.

For more information about providing remediation resources and configuring sandbox pages, see “Providing Remediation Resources for Users,” on page 104.

Figure 11-2: Endpoint Restriction Alert

2. If the user clicks the help link, the appropriate sandbox page for that enforcement rule type appears:

3. When the user becomes compliant the client no longer restricts the session, and the user can access the endpoint network.
Enforcement Rule Workflow

Use the Enforcement Manager to create rules to:

- Require or prohibit specific conditions, such as files, programs, or Windows Registry keys and values, on the endpoint computer
- Require specific antivirus programs and definition files on the endpoint computer
- Require a specific type and version of client on the endpoint computer

To manage your enforcement rules:

1. Plan your enforcement rules and remediation strategy.
   
   See "Enforcement Rule Workflow," on page 102
   
   a. Decide which rules you want to require or prohibit and what action you want the client to take. It is recommended that you begin by using rules that observe or warn users (instead of restricting them) so as to avoid disrupting your users. Later, you may decide to reconfigure some rules to restrict non-compliant users.
   
   b. Gather all the information and resource files that your users will need to become compliant with your rules. You will use this information when you customize your sandbox pages, and also when you specify remediation resources in the enforcement rules.
   
   c. Customize your sandbox pages with the appropriate resources.

2. Configure the heartbeat interval.

   The interval between compliance check settings is regulated by the number of heartbeats so, you may wish to adjust the heartbeat interval. “Configuring the Heartbeat Interval,” on page 118.

3. Configure your Policy.

   If you do not already have a security policy, create one. Then add enforcement rule functionality to your policy by creating and adding enforcement rules, and by configuring other, related policy settings.
   
   a. Create your policy.
      
      If you have not already created a security policy, do so now, otherwise, edit an existing policy. See "Managing Security Policies," on page 46.
   
   b. Enable enforcement rule alerts and logging.
      
      These settings control what alerts your endpoint users see and what events are sent to the reports. In the same tab, you can configure the custom text that is shown in the enforcement rule alerts. See "Enabling Enforcement Rule Alerts and Logging," on page 107.
   
   c. Create your rules.
      
      Using the information you gathered in step 1, create your rules, being sure to specify your remediation resources. When creating rules that restrict you
should specify the remediation resources necessary for compliance. If desired, you can configure Endpoint Security to apply remediation resources automatically. See “Enforcement Rule Workflow,” on page 102.

See:
- “Providing Remediation Resources for Users,” on page 104
- “Managing Enforcement Rules,” on page 108

For best performance, it is recommended that you create no more than 40 enforcement rules.

d. Add your enforcement rules to your security policy.
   In order for your rules to be enforced, you must add them to your security policy. You may also optionally group your rules at this point. See “Adding and Grouping Enforcement Rules,” on page 115.

e. Set your compliance check settings.
   Compliance check settings determine how long endpoint users can be out of compliance before their connection is restricted or terminated. See “Configuring Compliance Check Settings,” on page 117.

f. Set your restriction firewall rules.
   Restriction firewall rules determine the limits of access for restricted users. If you are using rules that restrict you must configure restriction firewall rules in order to limit non-compliant user access. See “Adding Restriction Firewall Rules to Your Policy,” on page 117.

g. Save your policy.

4. Deploy the policy and assign it to endpoint users.
   Before a policy can take effect, it must be deployed to endpoint users. See “Deploying Policies,” on page 49.

5. Monitor compliance.
   Use the compliance reports to monitor how well your endpoint users are complying with your enforcement rules. If many users are being terminated or restricted, you may need to temporarily use less restrictive rules and provide more remediation information. If users are generally in compliance, it may be time to increase your security by adding more and stricter rules. See “Tracking Enforcement Rule Compliance,” on page 119.
Minimizing Support Requirements

Enforcement rules can cut users off from the network resources they need when they are out of compliance. Therefore, it is important to provide easy means for the user to become compliant, thereby minimizing any support requirements related to enforcement rules.

Use the information in the following section to minimize the support burden:

- “Providing Remediation Resources for Users,” on page 104
- “Using Rules that Observe or Warn,” on page 105

Providing Remediation Resources for Users

When implementing enforcement rules, provide adequate resources and information in the enforcement alerts and sandbox pages to enable warned and restricted users to become compliant. There are two ways to configure remediation resources:

- In the enforcement rule, you can specify a remediation resource that users can download and install themselves. For restricted users, you have the option of configuring Endpoint Security to run remediation resources automatically. If you are using automatic remediation, the file you specify must be an executable.
- In the enforcement sandbox pages.

If you are using enforcement rules in conjunction with Cooperative Enforcement with a Gateway, you must provide remediation resources on the Endpoint Security server host itself using an uploaded file because restricted users will be unable to connect to any other network resources.

To configure remediation resources:

1. Identify which programs, files, registry keys, or other conditions you want to require or prohibit on endpoint computers to create a secure environment. Be sure to determine the correct information for each operating system.
2. Determine what information and resources non-compliant users need to become compliant. Some suggestions:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Configuration Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific details</td>
<td>Provide the specific conditions of the rule.</td>
<td>In an enforcement or antivirus provider rule, enter custom text that clearly describes the rule conditions with which the user may not be compliant. This text displays in the Alert and on the sandbox page.</td>
</tr>
</tbody>
</table>
Configure custom text and URLs in enforcement rules. Non-compliant users now have specific resources and information to help them become compliant.

Using Rules that Observe or Warn

An important strategy for smoothly implementing enforcement rules is to first create rules that observe or warn, but do not restrict non-compliant computers. This helps identify any frequently occurring non-compliant conditions in your network before restricting users as a result of those conditions.

Rules that Observe

When you configure an enforcement rule to observe, the client logs non-compliance events and reports them to the Endpoint Security server. The user session is not restricted.

Configure observe rules for centrally-managed software that users do not install themselves. This allows you to tell which users need the software without inconveniencing users with compliance issues they cannot solve for themselves.

Rules that Warn

When you configure an enforcement rule to warn, the client displays an Alert message that directs the user to remediation resources. The client logs the event, but allows the user full access to the endpoint network.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Configuration Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links</td>
<td>Include links to external sites where the user can download the necessary programs or files.</td>
<td>For links on the sandbox page to programs or files needed when a user is out of compliance with a specific rule, include the URL in the Enforcement Rule page. Note that you cannot automatically redirect a user to a link.</td>
</tr>
<tr>
<td>Executable Files</td>
<td>Configure Endpoint Security to remediate restricted endpoints by automatically running the necessary executable file.</td>
<td>Configure automatic remediation when setting up the enforcement rule or antivirus rule. The client can access the remedial file either directly or through an external URL.</td>
</tr>
<tr>
<td>Steps</td>
<td>Explain how to install and configure required resources.</td>
<td>On the sandbox page, provide detailed instructions that are specific to all enforcement rules.</td>
</tr>
<tr>
<td>Technical Support</td>
<td>Technical support contact phone number and/or e-mail addresses for your company.</td>
<td>Include this information in all sandbox pages.</td>
</tr>
</tbody>
</table>

Configure custom text and URLs in enforcement rules. Non-compliant users now have specific resources and information to help them become compliant.
Configure warn rules for software that users are responsible for installing and maintaining themselves.

**Tracking Rules that Warn or Observe**

After deploying a policy with an observe or warn rule, use the Enforcement Violations by Rule, Enforcement Violations by Policy, and Endpoint Status versions of the Endpoint Monitor Report to track the number of users affected by the rule. By tracking which users are non-compliant and the frequency of non-compliance, and by seeing how long it takes users to come into compliance, you can gauge the effectiveness of your policy and remediation resources.

To log enforcement-related events, configure the Client Alerts and Logging on the Client Settings tab of the security policy. (See “Enabling Enforcement Rule Alerts and Logging,” on page 107.)

When you are satisfied that your rule and resources will enhance security without unduly increasing your support burden, you may want to change the action indicator in the rule from Observe or Warn to Restrict and redeploy the policy. For rules that restrict, you can configure Endpoint Security to apply remediation resources automatically.
Enabling Enforcement Rule Alerts and Logging

This section explains how to:

- Configure the client to display the enforcement rule's custom alert on the endpoint computer.
- Configure the client to log events for use in reports.
- Specify custom text in the enforcement rule alerts.

To configure alerts and logging:

1. Go to the Client Settings page.
   
   For navigation information, see “Client Settings,” on page 191.

2. In the Client Alerts and Logs area, in the Enforcement alerts row, select:
   - Display to display an alert when the user is out of compliance with an enforcement rule.
   - Log to have the client record non-compliant events and report it to the Endpoint Security server.

3. Optionally, in the Custom Messaging area, type the custom message and link text that should appear in alerts.

4. Click Save.

   You deploy the policy for the settings to take effect.
Managing Enforcement Rules

This section explains how to create the following types of rules:

- “General Enforcement Rules,” on page 108
- “Antivirus Provider Rules,” on page 109
- “Client Enforcement Rules,” on page 112

You can create your enforcement rules in advance using the Policy Objects page or as you need them during policy creation. You can use the same enforcement rule in multiple policies.

This section also contains the following topics:

- “Editing an Enforcement Rule,” on page 113
- “Deleting Enforcement Rules,” on page 113

General Enforcement Rules

Use general enforcement rules to require or prohibit specific file or program configurations not covered by antivirus or client enforcement rules.

Creating a Program, File, or Key Enforcement Rule

General enforcement rules consist of the rule conditions, the type of check, the rule action, and remediation information.

To create a general enforcement rule:

1. Go to the Enforcement Rules Manager page.
   
   For navigation information, see “Enforcement Rules Manager,” on page 192.

2. Click New and select Enforcement Rule.

3. Name the rule, and configure the settings.
   
   For detailed information on the enforcement rule settings, see the online help.

   a. Configure the rule conditions.
      
      Set the conditions that are either prohibited or required on the endpoint computer.

   b. Set the type of check.
      
      General enforcement rules can either prohibit or require the conditions specified.
c. Set the rule action.
   The rule action determines what happens to endpoint users that are out of compliance with the rule.
   If you choose to restrict or warn the endpoint user, you should configure the custom text for this enforcement rule and provide a remediation resource. If you choose to restrict, you must configure restriction firewall rules for the policies that include this rule, or your users will not be restricted.

d. Set the remediation options for the rule.
   It is highly recommended that you set remediation rules to help your endpoint users to comply with your rules. For rules that restrict, you can configure Endpoint Security to remediate the endpoint automatically.
   The following is an example of custom text for a rule that prohibits a program:
   ‘XYZ program is installed on your computer. You must remove this program to regain full access to the network.’
   The custom text you specify is only available in the alert if you configure the client alert and logging settings to display enforcement rules on the Client Settings tab of the security policy.

4. Click **Save**.
   You must deploy the policy for the enforcement rule to take effect.
   To assign this rule to an endpoint user, add it to a security policy as described in “Using Enforcement Rules in a Security Policy,” on page 115.

**Antivirus Provider Rules**

Use antivirus provider rules to require endpoints to run a specific antivirus program. If the endpoint becomes non-compliant, the client can restrict the user session, warn the user without restricting, or observe the violation without restricting. You can specify a remediation resource that users can download and install themselves. For restricted users, you have the option of configuring Endpoint Security to run remediation resources automatically.

When creating an antivirus provider rule, you can either enter antivirus engine and DAT file information manually or use a reference client.

Manual configuration requires frequent maintenance to keep up with software and DAT file updates. You can automate your updates by specifying a single computer (called an antivirus reference client) to provide software and DAT file information to Endpoint Security. When you update the DAT file or antivirus engine on the reference client, Endpoint Security updates its antivirus provider rules accordingly.
To create antivirus provider rules manually, see “Creating an Anti-Virus Enforcement Rule,” on page 111.

**Using Reference Clients**

To avoid having to constantly update your software and DAT file configurations in your policy, you can configure an antivirus reference client and then specify that client as the standard in your enforcement rule.

Reference clients do not provide DAT file remediation to your endpoint computers. You should provide remediation resources in your policy.

If you are using Cooperative Enforcement with a gateway and are checking for compliance with enforcement rules, you must upload the DAT files as remediation resources because users that are restricted at the Gateway level will not be able to access other internal antivirus DAT file resources.

**To create antivirus enforcement rules based on a reference client:**

1. Set up your reference client computer.

   The reference client should be an endpoint computer that you know and trust to be free of malware with the desired antivirus software engine and DAT file. Do not assign a policy to the reference client computer. Be sure the intended reference client has the latest antivirus engine version and DAT file, and that it is connected to the Endpoint Security server.

2. Install a client on the reference computer.

   Clients on reference computers behave the same way as any other clients except that the antivirus information they send to the Endpoint Security server is used for enforcement. Do not assign the policy that uses the reference client to the reference client computer. Assign a policy without enforcement rules to the reference client computer.

Client versions 7.0 and higher use a different method to detect antivirus providers on endpoint computers than previous clients. It is highly recommended that you use the same version of the client on your reference client as you distribute to your other endpoint computers.

3. Configure Endpoint Security to use the antivirus reference client.

   a. Go to the **Antivirus Reference Clients** page.

      For navigation information, see “Antivirus Reference Clients,” on page 191.

      This page contains entries for all supported providers, whether or not reference clients are configured. Endpoint Security does not display antivirus software and DAT file details for a given provider until you configure a reference client.

   b. Select a provider from the list and click **Configure**.
c. Specify the reference client in one of the following ways:
   - To identify the client by IP address, select **IP Address** and type the address in the adjacent field. You must use a static IP address that is dedicated to the reference client.
   - To identify the client by custom user ID (CUID), select **CUID** and enter the path in the adjacent field.

d. Click **Save**.
   The reference client is now available for use in an anti-virus enforcement rule.

4. Create a new antivirus enforcement rule that uses information from the reference client.
   See “Creating an Anti-Virus Enforcement Rule,” on page 111.

### Creating an Anti-Virus Enforcement Rule

Perform the steps below in the Endpoint Security Administrator Console to create an antivirus enforcement rule for a supported provider.

**To create an antivirus enforcement rule:**

1. Go to the **Enforcement Rules Manager** page.
   For navigation information, see “Enforcement Rules Manager,” on page 192.
2. Click **New** and select **Anti-virus Rule**.
3. Name the rule, and configure the settings.
   For detailed information on the enforcement rule settings, see the online help.
   a. Enter the antivirus provider information.
   ![You may encounter time zone issues when using Symantec Antivirus or Trend Micro OfficeScan Corporate Edition and enforcing by DAT time.]
   b. Configure the rule conditions.
   c. Set the rule action.
   ![You may encounter time zone issues when using Symantec Antivirus or Trend Micro OfficeScan Corporate Edition and enforcing by DAT time. Enforce by version.]
The rule action determines what happens to endpoint users that are out of compliance with the rule.

If you choose to restrict or warn the endpoint user, you should configure the custom text for this enforcement rule and provide a remediation resource. If you choose to restrict, you must configure restriction firewall rules for the policies that include this rule, or your users will not be restricted.

d. Set the remediation options for the rule.
   It is highly recommended that you set remediation rules to help your endpoint users to comply with your rules. For rules that restrict, you can configure Endpoint Security to remediate the endpoint automatically.

The following is an example of custom text for a rule that require an antivirus program:

Trend Micro OfficeScan Corporate Edition is not installed on your computer. Please install this program to regain full access to the network.

The custom text you specify is only available in the alert if you configure the client alert and logging settings to display enforcement rules on the Client Settings tab of the security policy.

4. Click Save.

   You must deploy the policy for the enforcement rule to take effect.

   To assign this rule to an endpoint user, add it to a security policy as described in “Using Enforcement Rules in a Security Policy,” on page 115.

**Client Enforcement Rules**

Use client enforcement rules to require users to have a particular type and version of the client on the endpoint computer. This is recommended when performing minor client upgrades from one client to another. Generally, this is only recommended for minor release upgrades and. You can only use client enforcement rules to upgrade from a 6.x or higher version.

To encourage compliance when upgrading clients, it is recommended that you use the automatic upgrade option. This starts the upgrade with minimal input or disruption to the endpoint user.

**To create a client enforcement rule:**

1. Go to the Enforcement Rules Manager page.
   For navigation information, see “Enforcement Rules Manager,” on page 192.

2. Click New and select Client Rule.

3. Name the rule, and configure the settings.
   For detailed information on the enforcement rule settings, see the online help.
a. Configure the rule conditions.
   Choose the client you want your endpoint computers to have.

b. Set the rule action.
   The rule action determines what happens to endpoint users that are out of compliance with the rule.

   If you choose to restrict or warn the endpoint user, you should configure the custom text for this enforcement rule and provide a remediation resource. If you choose to restrict, you must configure restriction firewall rules for the policies that include this rule, or your users will not be restricted.

c. Set the remediation options for the rule.
   It is highly recommended that you set remediation rules to help your endpoint users to comply with your rules. For rules that restrict, you can configure Endpoint Security to remediate the endpoint automatically.

The following is an example of custom text for a client provider rule:

   Agent v. 7.0 is not running on your computer. You must have a current version of this program installed and running to regain full access to the network.

   The custom text you specify is only available in the alert if you configure the client alert and logging settings to display enforcement rules on the Client Settings tab of the security policy.

4. Click Save.
   You must deploy the policy for the enforcement rule to take effect.
   To assign this rule to an endpoint user, add it to a security policy as described in “Using Enforcement Rules in a Security Policy,” on page 115.

Editing an Enforcement Rule

The process of editing rules is similar to creating a new one (see “Creating a Program, File, or Key Enforcement Rule,” on page 108, “Antivirus Provider Rules,” on page 109, or “Client Enforcement Rules,” on page 112, for detailed instructions). When you edit a rule used by a security policy, the enforcement, antivirus, or client rule definition is also modified in the security policy. The modify settings are applied to the security rule the next time the policy is deployed.

Deleting Enforcement Rules

Deleting an enforcement, antivirus, or client rule completely removes the rule from Endpoint Security. These rules are also removed from security policies at the time that you delete them. The change to the security policy is applied the next time the policy is deployed.
To delete rules:

1. Go to the Enforcement Rules Manager page.
   For navigation information, see “Enforcement Rules Manager,” on page 192.

2. In the row for the enforcement rule, click Delete.
   A confirmation message appears.

3. Click Yes.
   The rule is deleted from the system and no longer appears in the enforcement rules list. The enforcement rule is removed from existing policies the next time you deploy it.
Using Enforcement Rules in a Security Policy

This section explains how to manage enforcement rules in a security policy. Assign enforcement rules to prohibit or require specific programs, files, and/or registry keys on the endpoint computer and determine the action taken when those conditions are met.

To add enforcement rules to the security policy, perform the steps in the following sections:

1. “Adding and Grouping Enforcement Rules,” on page 115
2. “Configuring Compliance Check Settings,” on page 117
3. “Adding Restriction Firewall Rules to Your Policy,” on page 117
5. “Configuring the Heartbeat Interval,” on page 118

Adding and Grouping Enforcement Rules

This section explains how to assign an enforcement or antivirus rule to a security policy and create enforcement and antivirus rule groups. The user's computer must be compliant with each rule and rule group in the security policy.

• “Adding Enforcement and Antivirus Provider Rules,” on page 115
• “Grouping Enforcement and Antivirus Provider Rules,” on page 116

Adding Enforcement and Antivirus Provider Rules

This section explains how to add enforcement and antivirus provider rules that you created in the Enforcement Manager or were configured in the System Domain to a security policy. The user's computer must be compliant with all rules in the policy. Use the Endpoint Security Administrator Console to add rules.

To add rules to a policy:

1. Go to the Enforcement Settings page.
   For navigation information, see “Enforcement Settings,” on page 192.
2. In the Enforcement Rules area, click Add.
3. Select the rules you want, then click Add.
   The Enforcement Settings tab appears with the enforcement rules in the policy.
   If you use restrict or warn enforcement or antivirus rules, you should configure the Enforcement Alert for this rule and provide remediation resources. If you use a restrict enforcement or antivirus rule, you should configure Compliance Check Settings and Restriction Firewall Rules for this policy. You must save and deploy the policy for the enforcement or antivirus rule to take effect. For more information
about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49. You can also optionally group enforcement and antivirus rules.

**Grouping Enforcement and Antivirus Provider Rules**

After you add enforcement rules (including antivirus provider rules) to a policy, you can create enforcement rule groups. When rules are grouped, the endpoint computer must be compliant with at least one rule in the group. Use the Endpoint Security Administrator Console to group your rules.

When grouping enforcement rules, note the following:

- The rule action for the entire group supersedes the rule actions of the rules in that group.
- Automatic remediation is disabled for rules in a group. Endpoint Security still provides the remediation resource in the sandbox, but the user has to apply the resource manually. If a rule in the group is used individually in a different policy, automatic remediation still works for the rule in that policy.
- You cannot add client rules to a group.

**To group enforcement rules:**

1. Go to the Enforcement Settings page. For navigation information, see “Enforcement Settings,” on page 192.
2. Select the rules you want to group and click Group. The rules you selected are combined into one row and a group title box appears.
3. In the group title box, type a name for the group.
4. Choose the action for the enforcement rule group:
   - **Restrict** - Restricts noncompliant users according to your restriction firewall rules
   - **Observe** - Allows noncompliant users access, and logs the violation
   - **Warn** - Alerts the user that their computer is not compliant, allows the user to access the network, and logs the violation
5. Click **Save** to save the new group.

For enforcement rules that warn or restrict, provide remediation resources and configure an Enforcement Alert for the group. Note that automatic remediation does not work for rules in a group. (See the note above for details.)
For enforcement rules that restrict, configure compliance check settings and restriction firewall rules for this policy.

You must save and deploy the policy for the rule group to take effect. For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.

### Configuring Compliance Check Settings

Compliance check settings to control how long a endpoint computer can be out of compliance with the enforcement rules for the policy before being restricted. The default number of heartbeats is four.

**To configure compliance check settings:**

1. Go to the Enforcement Settings page.
   
   For navigation information, see “Enforcement Settings,” on page 192.
2. Set the **Number of non-compliant heartbeats before restriction** setting.
3. Set the **Subsequent non-compliant heartbeats before termination** setting.
   
   You must save and deploy the policy for the new compliance check settings to take effect.

### Adding Restriction Firewall Rules to Your Policy

This section explains how to add restriction firewall rules to your policy. Restriction firewall rules limit access for users who are not compliant with enforcements rules that are set to restrict. Use restriction firewall rules to only allow your users access to the resources they need to become compliant. If you do not configure restriction rules, the users who are out of compliance will not be restricted. Use the Endpoint Security Administrator Console to add restriction firewall rules.

**To add restriction firewall rules to your policy:**

1. Go to the Enforcement Settings page.
   
   For navigation information, see “Enforcement Settings,” on page 192.
2. Select the firewall rules you want to use and click **Add**.
   
   If you need to create a new firewall rule, you can do so by clicking **New Firewall Rule**.
3. Click Add.

4. Use the up and down arrows to rank the restriction firewall rules.
   
   Rules are enforced according to their rank. Generally, you will want to create rules
to allow traffic to the areas you want the user to have access to, and then specify a
‘cleanup rule’ as the last rule, blocking all traffic.

   You must save and deploy the policy for the restriction firewall rules to take effect.
   For more information about saving and deploying your policy, see “Creating

**Configuring the Heartbeat Interval**

Since compliance check settings are regulated by the number of heartbeats, you may
wish to adjust the heartbeat interval. Use the Endpoint Security Administrator Console
to configure the heartbeat interval.

**To configure the heartbeat interval:**

1. Go to the **Client Configuration** page.
   
   For navigation information, see “Client Configuration,” on page 191.

   If you have not configured client settings, the **Client Configuration** page shows the
default settings.

2. Click **Edit**.

3. In the **Interval** field, enter the number of seconds you want to have between
   heartbeats.

   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. Typical heartbeat intervals range between 300
   and 1800 seconds.

4. Click **Save**.

   For more information about saving and deploying your policy, see “Creating
Tracking Enforcement Rule Compliance

Enforcement rules and enforcement settings let you restrict the network access of endpoints that do not run specified software (such as up-to-date antivirus software) or that otherwise fail to meet specified conditions (such as periodic spyware scans and treatments). Enforcement rules and settings can also restrict endpoints that are running undesirable or dangerous software.

Endpoint Security provides a variety of reports that help you monitor compliance with your enforcement rules and settings. You can view a general compliance report showing all enforcement events, as well specialized reports showing events by rule and by policy. A report showing historical enforcement events is also available. Use these compliance reports to analyze the effectiveness and user impact of your enforcement rules, and to help you troubleshoot specific support issues with restricted users.

An enforcement event occurs when a user violates an enforcement rule or an enforcement setting. If a user violates more than one enforcement rule or setting, each violation causes its own enforcement event.

When you first implement enforcement rules and settings, configure them to ‘observe’ endpoints (instead of restricting them). You can then view the compliance reports to monitor effects on end users. If endpoint user effects are not too great, you may decide to reconfigure some of your rules to restrict non-compliant endpoints.

Viewing Compliance Status

The Endpoint Status Report report shows which clients currently comply with your enforcement rules and settings, and which clients do not. Endpoint Security also provides reports that show enforcement rule violations organized by rule and by policy.

The Endpoint Status Report report divides clients into the following statuses:

- **Compliant**—the endpoint complies with all enforcement rules and settings.
- **Observe**—the endpoint violates one or more enforcement rules, but the rules are configured to record the violation without taking any other action.
- **Warn**—the endpoint violates one or more enforcement rules, but the rules are configured to warn the user.
- **Non-Compliant**—the endpoint violates one or more enforcement rules but has not yet been restricted or terminated.
- **Restricted**—the endpoint has violated a rule configured to restrict the user, and the user has subsequently failed to remediate the endpoint in the grace period. (The default grace period is four heartbeats, though you can configure the grace period in the policy.)
- **Terminated**—the endpoint has violated a rule configured to restrict the user, and the user has subsequently failed to remediate the endpoint in the allowed time. (The default time allowed is six heartbeats after restriction, though you can configure the allowed time in the policy.)
A client is unconnected when the endpoint computer is turned on, the user is logged in, and the endpoint computer is able to connect to the Endpoint Security server. It is therefore normal for a majority of endpoints to be unconnected during nonworking hours, when most users have turned off their computers.

If you have configured Office Awareness, the unconnected status does not necessarily indicate that the client is using the disconnected policy, or is in the disconnected state. In this circumstance, clients are shown in this report as unconnected when they miss a number of heartbeats to the Endpoint Security server. They are in the disconnected state when they are not on your network.

If you are not using Office Awareness, clients are in the disconnected state and use the disconnected policy when they are shown as unconnected in this report.

- **Unconnected**—the endpoint is not connected to the Endpoint Security server.

- **Shutdown**—The endpoint user has shut down the endpoint computer.

For navigation information for this report, see “Endpoint Status Report,” on page 192.

### Violations by Rule and Policy

The Enforcement Violations by Rule report displays rules that have been violated, with links to lists of endpoints that have violated each rule. The Enforcement Violations by Policy report displays policies containing rules that have been violated, with links to lists of non-compliant endpoints with those policies.

For navigation information for these reports, see “Enforcement Violations by Rule,” on page 192 and “Enforcement Violations by Policy,” on page 192.

### Viewing Antivirus Versions

Use the Antivirus Provider Brands Report to view the various antivirus applications that are currently in use in your organization.

For navigation information for this report, see “Antivirus Provider Brands Report,” on page 191.
Chapter 12
Protecting Against Spyware

In This Chapter

- Introduction to Antispyware Protection  page 121
- Antispyware Workflow  page 122
- Managing Antispyware Protection  page 123

Check Point Antispyware protects your network from threats ranging from worms and Trojan horses to adware and keystroke loggers. Use Antispyware to detect and treat spyware on your endpoint computers.

The Endpoint Security server regularly receives updated spyware definitions from a Check Point update server. You can use these definitions in policies to check your endpoint computers for spyware. You can also enforce regular spyware scans and set treatment options.

Antispyware is a feature that requires a license. See “Licensing,” on page 177 for more information.

Introduction to Antispyware Protection

Antispyware scans endpoints for spyware and treats any spyware applications it finds. It looks for known spyware file names and sizes in the areas you specify.

You can accept the default treatment and client notification or restriction settings, or modify the settings by spyware category. For example, you might configure a policy that deletes Trojans and then notifies end users of the deletion. After configuring treatment options, you can enforce regular spyware scans and treatments, and then observe, warn, or restrict endpoints that are not successfully scanned and treated at the appointed time. Your treatment parameters and enforcement settings become part of the policies you deploy to endpoints.
Scan Target Drives and Exclusions

Use target drives and exclusions to determine which directories and file types should be scanned.

To increase the efficiency of your scan, you can specify the parts of your endpoint computers that you want Antispyware to scan. For example, you can specify any local, removable, CD-ROM, or network drive as a target drive.

You may wish to exclude certain directories to save time when scanning, or exclude certain types of files, such as database files, from becoming corrupted. Use the Scan Exclusions feature to specify the directories and file extensions you do not want scanned.

The target drives and exclusions that you specify apply to both Antivirus and Antispyware.

Treatment Options

You can configure which action the client should take when a virus is detected. You can choose:

- **Automatic**—Performs the specified treatment without notifying the end user.
- **Notify**—Treats the spyware and then notifies the end user about the treatment. The end user cannot cancel the treatment. (This option works only for Flex users.)
- **Confirm**—Lets endpoint users specify the treatment. Endpoint users can choose:
  - **Allow** - Lets the spyware application run one time
  - **Always Allow** - Lets the application run at any time
  - **Quarantine** - Moves the application to a quarantine area
  - **Delete** - Deletes the file. This option works only for Flex users.

Antispyware Workflow

Endpoint Security enforces Antispyware settings through individual policies. Use the following steps to configure Antispyware:

**To configure Antispyware:**

1. License Antispyware.
   
   If you have not already done so, generate and apply your Smart Defense Antispyware licenses for endpoints and updates. See “Licensing” on page 177.
2. Check your ports.

For Antispyware protection to work correctly, Endpoint Security must have access to ports 80, and 443 to retrieve the latest spyware information. Make sure that your firewall allows this traffic.

3. Configure your proxy server.

If you plan to use Antispyware in an environment that includes a proxy server for Internet access, perform the configuration steps for using the Endpoint Security system with a proxy server, as described in “Proxy Configuration,” on page 184.

4. Configure your settings.

Use the Endpoint Security Administrator Console to enable Antispyware and configure your Antispyware settings in your policies. See “Configuring Antispyware Protection,” on page 124.

5. Set any exceptions (optional).

If necessary, you can allow certain spyware products to run. See “Allowing a Spyware Program to Run,” on page 124.

6. Set enforcement for Antispyware scans (recommended).

You can configure your policies to enforce regular scans and treatment on endpoint computers. Endpoint computers that do not run the scan, or do not treat spyware can be restricted. See “Enforcing Antispyware Scans and Treatments,” on page 125.

7. Configure updates.

In order to provide the most complete protection, Antispyware needs to obtain updates. You can set automatic updates or stage updates with a test group before deploying to all users. See “Managing Updates,” on page 132.


There are a number of ways to review Antispyware events on your endpoint computers. You can find out when your endpoints were last scanned, how many Antispyware events have taken place, and which users and which types of spyware have been involved. See “Monitoring Antivirus and Antispyware Activity,” on page 139 for details.

Events related to tracking cookies are not included in reports, as they are too numerous.

Managing Antispyware Protection

This section contains the following topics:

- “Configuring Antispyware Protection,” on page 124
Configuring Antispyware Protection

You must enable Antispyware protection to have access to the various configuration options. Your policies

To configure Antispyware protection in a policy:

1. Go to the Anti Virus/AntiSpyware page. For navigation information, see “Anti Virus/AntiSpyware,” on page 191.
2. Select Protect against spyware. The Antispyware settings are now accessible.
3. Configure the Antispyware settings. Configure the following settings:
   a. Set the time and date for the scan
   b. Modify the spyware treatment settings (optional). Endpoint Security divides spyware into several categories, such as adware, keystroke logger, and remote administration tool (RAT). Default scan settings quarantine all spyware and then notify the endpoint user. You can modify the default treatment settings for any or all spyware categories.
   c. Set the Scan Targets and Exclusions. These options apply to both Antispyware and Antivirus scans.
   d. Set the Treatment Options. Endpoint Security divides spyware into several categories, such as adware, keystroke loggers, and remote administration tools (RAT). Default scan settings quarantine all spyware and then notify the endpoint user. You can modify the default treatment settings for the various spyware categories. You can only allow or delete tracking cookies automatically, since they are so numerous. For detailed information about these settings, see the online help.
4. Click Save. You must deploy the policy for the changes to take effect.

Allowing a Spyware Program to Run

This section explains how to allow individual spyware programs to run.
To allow a specific spyware program:

1. In the Treatment Settings table, do one of the following to find the desired program:
   - Click a category link to see the known programs in that category, and scroll through the list.
   - Type the application name and/or select the spyware category to search for, and click Search.
2. When you locate the program, select the check box in the Always Allow column next to the application name.
3. If you want to clear the search results or return to the category list, click the Back button.
4. Click Save.

Enforcing Antispyware Scans and Treatments

You can configure Endpoint Security to enforce regular spyware scans and treatments on endpoint computers. An endpoint is considered to be non-compliant with the scan enforcement if the user refuses or interrupts the scan or if the client fails to treat one or more spyware items. Non-compliant endpoints can be restricted from the network.

A scan is successful if the client treats all detected spyware applications. If any spyware applications remain untreated, the scan is not considered successful and does not satisfy enforcement requirements. Scans are considered successful, however, if Flex users intentionally allow a suspected spyware application.

You may want to initially configure Antispyware without enforcement to minimize user disruption. Later, you can add enforcement to your policies to increase user compliance. You can use the monitoring tools to gauge spyware activity, events, and user scan compliance. See “Monitoring Antivirus and Antispyware Activity,” on page 139.

To enforce Spyware scans and treatments:

1. In the Spyware Scan Settings section, select Restrict clients that don't comply with the Spyware Scan settings.
2. Click Save.

Endpoints that are not successfully scanned at the scheduled time are restricted according to the enforcement rules you created. For more information about restriction enforcement rules and their impact on the user, see “What a Restricted User Experiences,” on page 100.
In This Chapter

Introduction to Antivirus Protection  
Configuring Antivirus Protection  

Check Point Antivirus allows you to provide centrally-managed protection against virus risks to your endpoint computers. This chapter contains information about administering Antivirus. Antivirus is a feature that requires a license. See “Licensing,” on page 177 for more information.
Introduction to Antivirus Protection

The Antivirus feature keeps known and unknown viruses from affecting your endpoint computers by scanning files and comparing them to a database of known viruses and against a set of characteristics that tend to reflect virus behavior.

Depending on your settings, files are scanned as they are:
- Opened, closed, or executed
- As part of a full computer-wide scan

If a virus is detected, the client can render it harmless, either by repairing or denying access to the infected file.

There are also a number of ways to review Antivirus events on your endpoint computers. You can find out when your endpoints were last scanned, when they were last updated, and how many Antivirus events have taken place. See “Monitoring Antivirus and Antispyware Activity,” on page 139 for details.

This section contains the following topics:
- “Scan Methods,” on page 127
- “Scan Target Drives and Exclusions,” on page 128
- “Treatment Options,” on page 128

Scan Methods

When you turn on Antivirus in a policy, heuristic and on-access scans are always performed automatically on files. You can also schedule rigorous deep scans for previously unprotected endpoints.

Automatic Virus Scans

Heuristic Virus Scanning

In Antivirus heuristic scanning, files are scanned and infections are identified based on certain behaviors that are characteristic of viruses.

On-Access Virus Scanning

The Antivirus on-access scanning protects endpoint computers from viruses by detecting and treating viruses that may be dormant. On-access scanning supplies the most active form of virus protection. Files are scanned for viruses as they are opened, executed, or closed, thereby allowing immediate detection and treatment of viruses. An On-Access scan will only scan for viruses in an archive (compressed file, such as those with a .zip extension.) when the file is opened. Unlike other types of files, archives are not scanned when moved from one location to another.
Optional Virus Scans

Deep Scan

In addition to the automatic and optional Antivirus scans described above, you can schedule Antivirus to run a very detailed scan of every file on the Scan Targets you select.

Because it is so rigorous, the scheduled deep Antivirus scan has a significant impact on endpoint performance. For this reason, these scans are recommended for previously-unprotected endpoints, and are best run when your endpoint users are not using their computers.

Scan Target Drives and Exclusions

Use target drives and exclusions to determine which directories and file types should be scanned.

To increase the efficiency of your scan, you can specify the parts of your endpoint computers that you want Antivirus to scan. For example, you can specify any local, removable, CD-ROM, or other drive as a target drive.

You may wish to exclude certain directories to save time when scanning, or exclude certain types of files, such as database files, from becoming corrupted. Use the Scan Exclusions feature to specify the directories and file extensions you do not want scanned.

The target drives and exclusions that you specify apply to both Antispyware and Antivirus.

Treatment Options

You can configure which action the client should take when a virus is detected. You can choose:

- **Repair** - Choose this option to have the client attempt to automatically repair the endpoint computer without alerting the user. If the client is unable to repair the file, it will either quarantine the file, or ask the user, depending on which repair option you choose.

- **Ask the endpoint user** - Choose this option to ask the endpoint user which course of action to take. The client will display an alert, asking the user to choose from the following repair options:
  - **Repair**: Tries to repair the selected file.
  - **Rename**: Renames the file. By renaming a file, a user can avoid having to further alerts for this file.
  - **Quarantine**: Moves the application to a quarantine area
- **Delete**: Deletes the selected file. If necessary, the deletion will take place upon the next reboot of the computer.
Configuring Antivirus Protection

The following sections describe the best practices for using Antivirus. This chapter gives general instructions for configuring Antivirus. For details about the administrator console, see the online help.

To configure Antivirus:

1. License Antivirus.
   If you have not already done so, generate and apply your Antivirus license. See “Licensing Workflow,” on page 178.

2. Configure your proxy server.
   If you plan to use Antivirus in an environment that includes a proxy server for Internet access, perform the configuration steps for using Endpoint Security with a proxy server, as described in “Proxy Configuration,” on page 184.

3. Configure your settings.
   Use the Endpoint Security Administrator Console to configure your antivirus settings in your policies. See “Configuring Antivirus Settings,” on page 130.

4. Configure updates.
   In order to provide the most complete protection, Antivirus needs to obtain updates. You can set automatic updates or stage updates with a test group before deploying to all users. See “Managing Updates,” on page 132.

5. Monitor your results.
   Use the reporting features to monitor what types of viruses have been treated and how often your users are scanning and getting updates. See “Monitoring Antivirus and Antispyware Activity,” on page 139.

Configuring Antivirus Settings

You can use configure Antivirus settings in your policies. You must have the Antivirus administrator role in order to make Antivirus settings.

If endpoint users are running a third-party antivirus program, the client will detect it and disable on access scanning to avoid compatibility problems. To determine if your endpoints are using third-party antivirus programs, see the Antivirus Provider Brands Report. See “Viewing Antivirus Versions,” on page 120.

To configure Antivirus Settings

1. Go to the Anti Virus/AntiSpyware page.
   For navigation information, see “Anti Virus/AntiSpyware,” on page 191.
2. Select **Protect against viruses** to enable Antivirus in the policy.

3. Configure the following:
   - Antivirus Scan Settings
   - Scan Targets and Exclusions
   - Treatment Settings

   Refer to the online help for information about settings.

4. Click **Save**.

5. Assign and deploy the policy to have your changes take effect.

6. To see how many of your users are using Antivirus, see the Antivirus Provider Brands Report. For navigation information, see "Antivirus Provider Brands Report," on page 191
In This Chapter

Introduction to the Updates Feature
Making Updates Instantly Available
Configuring Automatic Client Updates
Configuring Client Update Staging
Deploying or Rejecting Previewed Updates
Offline Updates

Introduction to the Updates Feature

Use the Updates feature to receive, manage, and deploy:

- **Virus definition updates** - These updates ensure your endpoints are constantly protected against new viruses. The updates include DAT files, which are libraries of virus signatures.

- **Spyware definition updates** - These updates help to protect your endpoints against the latest spyware.

Using the Updates feature, you can:

- **View available updates** - By default, the Endpoint Security server receives the update information hourly from the Check Point update server, and makes it available for retrieval by your endpoints. The update is listed on the Home page and the Client Updates page.

- **Specify an automatic client updates schedule** - You can specify a schedule for how often the Endpoint Security server makes the latest update available for endpoint retrieval. (This feature creates automatic deployment, and does not allow you to test each update on a smaller group.)

See “Configuring Automatic Client Updates,” on page 136.
Preview updates with a test group - You can deploy client updates to selected endpoints for testing before rolling the updates out to all clients. This feature, called staging, allows you to update a select group of test endpoints. You can then determine if an update is acceptable to you before choosing to deploy it. (With this option, there is no automatic deployment of updates.)

See “Configuring Client Update Staging,” on page 136.

Immediately deploy client updates - At any time, you can choose to immediately make the latest collection of client components available to all clients. This is particularly useful if a virus outbreak occurs.

See “Making Updates Instantly Available,” on page 135.

**Update Delivery Process**

In order to protect your endpoint computers from the most recent viruses and spyware, the client must have the most up-to-date virus and spyware definitions (DAT files). The Update Server has the most recent definitions.

The process by which updates are delivered is shown in “Update Process,” on page 133.

![Update Process Diagram](image-url)

**Figure 14-1:** Update Process

The Update delivery process:

1. DAT files are updated on the external Check Point Update Server as needed.
2. The Endpoint Security server contacts the Update Server once an hour and receives DAT file information.

The Endpoint Security server only receives version information about the current DAT files. It does not receive the actual DAT files.

You will see traffic to the following locations:

- Antivirus update server - http://kav-integrity.zonelabs.com/

3. If you have configured offline updates, the Client contacts the Update Server at scheduled times or intervals and retrieves updates, if available.

If offline updates are configured, the Endpoint Security server relays only the location of the Update Server to the client via the policy. The client receives the engine and DAT files directly from the Update Server, not from the Endpoint Security server.

4. During synchronization, the Endpoint Security server relays the updates to the client.

During synchronization, the client informs the Endpoint Security server of its current DAT file versions.

Endpoint Security uses this information to create the update report.

For information about how you can view, test, and manage DAT updates, see “Managing Updates,” on page 132.

Update Staging Process

When you choose to preview updates, they follow a set path from release by Check Point to deployment on your endpoints, and you control when and if deployment happens. This path is a three-phase succession: updates remain at each stage until the update in front has moved forward down the path.

The current phase, or status, of each update is displayed in two places:

- The DAT File Updates table on the Home page
- The DAT File Updates table on the Client Updates page

The three phases of the client updates lifecycle are as follows:

1. **Available for Staging** - Endpoint Security server has been informed of a new update available from Check Point. It is listed on the Home page and on the Client Updates page. To move the available update to the Staging phase, click the Deploy to Staging link.

2. **In Staging** - The client update has been made available to a test user group. This phase applies only if you have chosen to manually preview client updates. At this point you can do either of the following:
   - Deploy the update to all endpoints by clicking the Deploy to Production link.
Deny deployment by clicking the **Deploy to Staging** link to replace this update with the next update for the test group.

See “Configuring Client Update Staging,” on page 136 and “Deploying or Rejecting Previewed Updates,” on page 137 for more information.

3. **In Production** - The update has been released for endpoint retrieval. All of your endpoints will retrieve this component when they check in with the Endpoint Security server.

### Making Updates Instantly Available

This update deployment method is especially useful if a virus outbreak is detected. At any time, you can view and manually deploy client updates without previewing them in a test group or waiting for the next scheduled deployment.

Because this method makes the updates available, but does not require clients to synchronize, it may take up to an hour for all your endpoints to get the update.

**To make client updates available:**

1. **Configure your proxy settings.**
   
   In order to obtain updates, Endpoint Security must be able to contact the Update Server. If you use a proxy server, you must allow this traffic. See “Proxy Configuration,” on page 184.

2. **Go to the Home page.**

   View available update components in the **DAT File Updates** table. It displays the version, date, and status for each available update.

   If you wish to check for a more recent update than the one displayed, click the **Check for Updates** link.

3. **Click the Deploy link in the Status column of the Client Updates table.**

   The status of the available DAT file changes to Deployed. It is immediately made available for all clients, regardless of the configured update schedule.

In the same manner, you can also instantly deploy client updates from the **DAT File Updates** table on the **Client Updates** page. For navigation information, see “**Client Updates,” on page 191.**
Configuring Automatic Client Updates

Use the following steps to configure how often the Endpoint Security server automatically makes updates available for endpoints. By default, unless manual previewing (staging) is configured, client updates are deployed for endpoint retrieval on an hourly basis.

This procedure should be used only if you do not wish to preview or test client updates before making them available.

**To configure automatic client updates**

1. Configure your proxy settings.
   In order to obtain updates, Endpoint Security must be able to contact the Update Server. If you use a proxy server, you must allow this traffic. See “Proxy Configuration,” on page 184.
2. Go to the Client Updates page.
   For navigation information, see “Client Updates,” on page 191.
3. In the DAT file updates section, click Schedule Automatic DAT File Updates.
4. Select an update frequency from the Schedule drop-down list.
5. Click Save.
   For more details about configuration options, see the online help.

Configuring Client Update Staging

This section describes the steps for setting up manual previews of Client Updates. This configuration allows you to preview updates within a test group before making them available to all endpoints.

**To Configure Manual Client Update Staging:**

1. Go to the Client Updates page.
   For navigation information, see “Client Updates,” on page 191.
2. Choose Manually Preview Anti-Virus Updates.
3. Configure a Test Group to receive the preview Antivirus Files, see “Configuring a Test Group,” on page 137.
4. In the Anti-Virus Updates Files table, click the Fetch link in the Status column. The DAT update is made available to your test group.
   Now you can check the results of the update on your test group before you make it available for all your endpoints.
Configuring a Test Group

The Endpoints report gives information about the endpoints that have connected to the Endpoint Security server. Use this report to view the status of a particular endpoint and also to add users to the test group for client updates. See “Managing Updates,” on page 132.

**To Configure a Test Group:**

1. Go to the **Endpoints Report** page.
   
   For navigation information, see “Endpoints Report,” on page 192.

2. Leave all the fields blank, and click **Apply Filter**.

3. In the User column, click the **Assign to Test Group** link under each endpoint that you want to add to the Test Group.
   
   (Once assigned, you can delete a user from the test group by clicking the **Remove from Test Group** link.)

   For more details about configuration options, see the online help for the **Client Updates** page.

Deploying or Rejecting Previewed Updates

Once you are aware of the results of an update on the test group, use the following steps to take either of these actions:

- If it is acceptable, make the update available to all endpoints.
- If it is not acceptable, reject the update and request the next one.

**To preview and deploy client updates:**

1. Go to the **Client Updates** page.

   For navigation information, see “Client Updates,” on page 191.

2. Depending on the action you want to take, perform the appropriate step:

   - To make the previewed DAT update available to all endpoints, click **Deploy**.
     
     The status of the previewed DAT update changes to Deployed. It is retrieved by all of your endpoints the next time they check in with the Endpoint Security server.

   - To reject the previewed DAT update and retrieve the next available update for your test group, click **Fetch**.

   For more details about configuration options, see the online help for the **Client Updates** page.
Offline Updates

Offline updates provide remote users with a way to get Antivirus updates without being connected to your corporate network. Users can get updates from your company’s server, or they can receive updates directly from Check Point Software.

To Set Up Offline Updates:

1. Go to the Client Updates page.  
   For navigation information, see “Client Updates,” on page 191.
2. Select Provide offline users access to Anti-Virus Updates.
3. If you are using a proxy server for internet access, make sure you allow traffic to the appropriate update server:
   - Antivirus update server - http://kav-integrity.zonelabs.com/
   See “Proxy Configuration,” on page 184.

When the endpoint computers connect to the server, they automatically receive the latest Antivirus files.

Your users must be using the most current version of the Antivirus software in order to use Check Point’s server.
Chapter 15

Monitoring Antivirus and Antispyware Activity

In This Chapter

- Monitoring Infection Activity on Connected Endpoints  page 139
- Monitoring Spyware and Virus Event History  page 140
- Monitoring Infection Scan and DAT Update Status  page 140

A critical part of centrally managing the protection of your endpoints is staying abreast of the virus and spyware events detected and handled by Endpoint Security. You can quickly find out about threats that have been detected and threats that have been resolved. You can also determine when your endpoints were last scanned and updated with the latest protections.

Events related to tracking cookies are not included in reports, as they are too numerous.

Monitoring Infection Activity on Connected Endpoints

The Home page tells you how many virus and spyware infections are active or resolved on your connected endpoints. The Infection Events page provides detailed information based on the type of infections.

To monitor the infection status of connected endpoints:

1. Go to the Home page.
2. View the Connected Endpoint Infections section on the Home page.
   This section displays the following:
- **Antivirus - Resolved Detections** and **Antispyware - Resolved Detections**: Lists resolved virus and spyware occurrences on the endpoints that have contacted the server in the last hour. Displays the number of files that were found infected and were successfully treated.

- **Antivirus - Unresolved Infections** and **Antispyware - Unresolved Infections**: Lists the number of infected files that have not yet been successfully treated.

3. Click a number in the right column to go to the *Infection Events* page for more details, including a breakdown by infection.

See the online help for more information about page contents.

### Monitoring Spyware and Virus Event History

Use the Infection Summary page to see how many infections were detected and treated successfully in a given time frame. By using the search options and links provided, you can also find out exactly which viruses and spyware were detected and treated.

**To monitor the infection history of all endpoints:**

1. Go to the *Infection History Reports*.
   
   For navigation information, see “*Infection History Reports,*” on page 192.

2. Choose a time span from the *Time Span* menu.

3. Choose from the *Event Type* menu.
   
   You can view a summary of all events or specify Antivirus or Antispyware.

4. Click *Apply Filter*.

   For more information about this page, refer the online help.

The Infections Summary page also provides the *Portal* button so that you can launch SmartPortal for more event reporting. Refer to the SmartPortal documentation for usage information.

### Monitoring Infection Scan and DAT Update Status

Use this monitoring feature to determine how often your endpoints are being scanned for viruses and spyware, to see if there are any that have not been scanned, and to check on the DAT update status of the endpoints.
To see a scan or update status report:

   For navigation information, see “Endpoint Monitor Report,” on page 192.

2. From the Chart menu, choose any of the following Reports:
   - **Check Point Antivirus Scanned Date Report** or **Check Point Spyware Scanned Date Report**: Shows when your endpoint computers were last scanned for viruses or spyware. If you find that your endpoints are not being scanned sufficiently often, you may need to use the enforcement feature to require they be scanned.
   - **Antivirus Provider Brands Report**: Click Check Point Endpoint Security Antivirus to see which versions of the virus definitions files your users have. If your users do not have recent DAT updates, they will not be protected against the most recent viruses.

3. To see a list of endpoints in a particular category, click the appropriate link in the legend.
   For example, in the Spyware Scanned Date chart, click the 48 hours link to see which clients have been scanned in the last 48 hours.
Chapter
Using SmartDefense

In This Chapter

Introduction to SmartDefense page 143
Configuring SmartDefense in a Policy page 144
Monitoring SmartDefense Events page 145

Employ SmartDefense to provide your enterprise with protection from several forms of network attacks. These attacks are characterized by the misuse of allowed traffic and services, and have the potential to cripple a network and cause Denial of Service (DoS) conditions that block endpoint access to hosts and servers.

The version of SmartDefense that is included in Endpoint Security is R55.
Introduction to SmartDefense

SmartDefense creates a framework of defense against attacks that are intended to harm the network by flooding it. You activate SmartDefense on your network by enabling it in the policies you deploy to your endpoints. While endpoint users are not allowed to configure SmartDefense, they do have the option of viewing SmartDefense logs with the client Alerts and Logs feature.

When SmartDefense protections are in place on your network endpoints, the network is protected from the following attacks:

- Ping of Death
- Tear Drop
- LAND
- Large (Max) Ping
- Malformed ANI
- CIFS worm catcher
- SQL slammer
- HTTP worm catcher
- HTTP header rejection

For information about each of these protections, please refer to the Smart Defense Protections Reference Guide NGX manual. For more details about SmartDefense and how it works, please refer to the FireWall-1 and Smart Defense NGX (R55) manual. You can download both of these documents from the Check Point Web Site.
Configuring SmartDefense in a Policy

This section describes how to configure SmartDefense in your policies.

To configure SmartDefense in a policy:

1. Go to the SmartDefense page.
   For navigation information, see "SmartDefense," on page 194.
2. Select Turn SmartDefense Protections ON for this policy.
3. Click Save.

Endpoint users will not receive the new policy until you deploy it. For more information about saving and deploying your policy, see "Creating Policies," on page 49 and "Deploying Policies," on page 49.
Monitoring SmartDefense Events

Whether you choose to act on attacks or only to observe them, events are tracked when SmartDefense is enabled.

As the administrator, you can view a report showing detected attacks and subsequent treatments in SmartPortal. The required portion of SmartPortal is included with Endpoint Security.

To check for SmartDefense incidents:

1. Go to the Endpoints Report page.
   For navigation information, see "Endpoints Report," on page 192.
2. Click View Events.
   SmartPortal launches and displays traffic logs.
3. Use the filter to view only SmartDefense events:
   a. Click the Filter button.
   b. In the dialog that appears, select the Event Type checkbox.
   c. In the Value field, enter SmartDefense.
   Only SmartDefense events are displayed, and columns that are not relevant to SmartDefense are empty.
   See the SmartPortal documentation for more information about filtering and using reports.
Chapter 17

Preventing E-mail Attacks

This chapter explains how to prevent your endpoint computers from participating in e-mail attacks using Mailsafe. Mailsafe limits outgoing e-mail to prevent e-mail worms and other malicious code from using the endpoint computer to send messages. MailSafe prevents endpoint computers from sending suspiciously large numbers of e-mails in short intervals and from sending e-mails to unusually large numbers of recipients. E-mail operations that exceed your specified limits trigger a warning to the endpoint user.

MailSafe works only with the SMTP protocol.
Managing Mailsafe Protection

To configure Mailsafe protection:

1. Go to the Messaging Settings page.
   For navigation information, see “Messaging Settings,” on page 193.
2. Configure the settings.
   For more information about these settings, see the Endpoint Security Online help.
3. Click Save.
   For more information about saving and deploying your policy, see “Creating Policies,” on page 49 and “Deploying Policies,” on page 49.
Chapter 18

Gateways and Cooperative Enforcement

In This Chapter

Introduction to Cooperative Enforcement page 149
Supported Gateways and Clients page 150
Configuring Cooperative Enforcement page 151

This chapter describes the Cooperative Enforcement™ feature of Endpoint Security.

If you previously integrated the client and Check Point VPN-1 SecureClient for the purpose of Cooperative Enforcement, be aware that you can now achieve similar enforcement goals with Endpoint Security and enforcement rules. (Note the following exception: There is no enforcement rule that you can use to run a third-party script.)

Endpoint Security provides a faster, simplified method of configuring and deploying VPN in packages, and provides endpoint users with a unified interface for the Endpoint Security client and VPN. You can still use the Endpoint Security client and SecureClient separately, but doing so does not take advantage of the simplified client management and unified interface. For details, see “VPN Options,” on page 158.
Introduction to Cooperative Enforcement

Use the Cooperative Enforcement feature to ensure that endpoint computers remotely connecting to your network:

- Are running a client.
- Have a specific policy.
- Comply with the Enforcement Rules in the security policy assigned to them.
- Are regularly contacting the Endpoint Security server.

Using this feature, you can restrict or terminate the gateway session for endpoint computers that are out of compliance, as well as endpoints that have stopped contacting the Endpoint Security server.

Cooperative Enforcement differs from enforcement with just Enforcement Rules in that it restricts at the gateway level. If you use Enforcement Rules alone, restriction happens at the client level.

You can configure Cooperative Enforcement to check for compliance with Enforcement Rules, but the restriction in this case occurs at the gateway level.

The enforcement action is activated after either of the following:

- **Four heartbeats of noncompliance.** By default, enforcement is activated after four heartbeats of noncompliance. You can change this number. For details, see “Configuring Compliance Check Settings,” on page 117.
- **Four missed heartbeats.** Enforcement is activated after four heartbeats are missed. This number cannot be altered.

A heartbeat lasts one minute by default, so if an endpoint has been out of compliance or has not contacted the server for four minutes, the client executes the action specified in the enforcement rule.

You can change the duration of a heartbeat. See “Configuring the Heartbeat Interval,” on page 118 for details.

If you are using a Check Point InterSpect™ or VPN-1 UTM/Power gateway, you can also have intra-LAN Cooperative Enforcement. See the *Endpoint Security Gateway Integration Guide* for more information.
Supported Gateways and Clients

For information about which gateways and clients are supported, see the Endpoint Security System Requirements Document.

If you use an unsupported gateway, Endpoint Security can monitor client events and the user status, but it will not be able to restrict access at the gateway level. You must use Enforcement Rules in conjunction with Restriction Firewall rules to restrict endpoint users. See “Enforcing Endpoint Security,” on page 97.
Configuring Cooperative Enforcement

This section lists the procedures you must perform to configure Cooperative Enforcement. For most supported gateways, you must configure Endpoint Security first, and then configure the gateway. The exception is the Check Point InterSpect gateway, which you must configure before you configure Endpoint Security.

Check Point InterSpect or VPN-1 UTM/Power Gateway Users:
If you are setting up Cooperative Enforcement using either of these gateways, see the Endpoint Security Gateway Integration Guide for full configuration instructions. Configuration for these two gateways is unique in the following ways:

- You do not need to add a group to the gateway
- You do not need to assign a policy to the gateway
- For InterSpect, you configure the gateway first, as outlined in the Endpoint Security Gateway Integration Guide, and then configure the Endpoint Security server.

To configure Cooperative Enforcement:

1. If you are using an 802.1x-compatible gateway, configure 802.1x settings in the Endpoint Security Administrator Console:
   a. Go to the Gateway Manager page. For navigation information, see “Gateway Manager,” on page 192.
   b. Click Edit.
   c. Configure the settings. For more information about completing the fields, see the online help.
   d. Click Save.
2. Add the gateway to Endpoint Security.
   See “Adding Gateway Catalogs,” on page 152. This step allows the Endpoint Security server to communicate with your gateway device.
3. Add groups to the gateway.
   You must add a group to your gateway catalogs (except InterSpect and VPN-1 UTM/Power gateway catalogs), and this group must have a specific name. You can add multiple groups to Cisco gateway catalogs, but other gateway catalogs must contain only one group.
4. Create and assign policies.
   a. Create your policies. If you want to enforce for the presence or absence of certain software on the endpoint computer, you must configure Enforcement
Rules in the policy. For more information about configuring enforcement rules, see “Enforcing Endpoint Security,” on page 97.

Enforcement rules are commonly used to require antivirus software on the endpoint computer. If you are using antivirus enforcement rules in your policy with Cooperative Enforcement, be aware that you will have to provide the DAT files as a remediation resource, because your restricted endpoint users will have no access to any internal sites except the Endpoint Security server. For more information, see “Providing Remediation Resources for Users,” on page 104.

If you are using Cooperative Enforcement, it is recommended that you not set any Restriction Firewall Rules in the Enforcement Rules of your policy. Using Cooperative Enforcement and Restriction Firewall Rules simultaneously makes it difficult to troubleshoot your configuration.

If you must use Restriction Firewall Rules in your policy, it is recommended that you begin with a policy that has no Restriction Firewall Rules and then, with each successive policy, add only one rule at a time. After you deploy each policy you should carefully observe the results before adding another rule.

For more information about Restriction Firewall Rules, see “Adding Restriction Firewall Rules to Your Policy,” on page 117.

b. Assign your policies.

You can assign policies to a group within the gateway and/or to the gateway itself. You do not assign security policies directly to Check Point VPN-1 UTM/Power or Check Point InterSpect gateways. Instead, you can create a catalog that contains the users or endpoints you want the gateway to monitor, and then assign a policy to the catalog. Or, allow the users to receive a policy according to policy inheritance.

5. Configure the gateway to complete integration of it with Endpoint Security.

For information specific to your gateway type, see the appropriate chapter of the Endpoint Security Gateway Integration Guide.

Adding Gateway Catalogs

Use the Endpoint Security Administrator Console to add gateway catalogs to Endpoint Security, which allows the Endpoint Security server to communicate with your gateway device. The first time a new user connects to the Endpoint Security server, they are dynamically added to the gateway catalog or group.
To add a new gateway catalog:

1. Go to the Gateway Manager page, click New Gateway and select your gateway type.
   For navigation information, see “Gateway Manager,” on page 192

![For all Cisco ASA and Concentrator gateways, choose Cisco VPN Gateway.]

2. Complete the fields with the appropriate information for your gateway.
   For explanations of the fields, see the online help.

3. Click Save.

4. To make sure that clients can access the gateway and therefore Endpoint Security, add the gateway to the Trusted Zone for a policy, and include the policy as an initial policy:
   a. Create a policy that includes the gateway's IP address in the Trusted Zone.
      See “Defining Zones,” on page 60 and “Managing Security Policies,” on page 46 for information on creating policies and Trusted Zones.
   b. Go to the Client Settings page.
   c. Click the Advanced button.
   d. Under Client Arbitration Settings, select Enterprise policy Trusted Zone overrides personal policy Trusted Zone.
   e. When you create the installation package, select the policy from the Initial Policy drop-down menu.
   f. Deploy the policy to the endpoint computers.
   These final steps help ensure that clients are able to access the gateway before their first policy download from the Endpoint Security server.

Adding Gateway Groups

You can add multiple groups to Cisco gateway catalogs, but other gateway catalogs must contain only one group. (The exceptions are the InterSpect and VPN-1 UTM/Power gateways, to which you do not need to assign a group.)

Adding groups to Cisco gateway catalogs, allows you to assign different policies and administrators to subsets of users within the gateway. If every user in the Cisco gateway is going to receive the same policy or be managed by the same administrators, you do not need to add groups.
To create a group:

1. Go to the Gateway Manager page.
   For navigation information, see "Gateway Manager," on page 192
2. Click the name of the gateway.
3. Click New Group.
4. In the Group Name box, type a name for the group.
   For the Cisco VPN 3000 Series concentrator, one group name must match the
   name defined on the concentrator.
5. Click Save.
Chapter 19
Client Installation Packages

In This Chapter

Introduction to Client Installation Packages page 156
Planning Your Client Distribution page 157
Client Package Workflow page 166
Managing Client Packages page 167
Monitoring page 171

Use this chapter to create and deliver client installation packages to protect endpoint computers.

This chapter describes only the client distribution administration tasks that are performed using the Endpoint Security Administrator Console. For more information about clients and how to deploy them to endpoint computers, see the Endpoint Security Client Management Guide.
Introduction to Client Installation Packages

Client packages provide a convenient way to install clients on your endpoint computers. Use client packages to install client programs along with configuration information and, optionally, security policies. Client installation packages consist of the following:

- **client.msi** - This file installs the client on your endpoint computer. The executable that is included is determined by the choice you make when create your package.

- **config.xml** - This file provides connection information that the client will use to communicate with the Endpoint Security server. It also configures some aspects of how the client is presented to the endpoint user and sets the Custom User ID, if specified. This file is configured by the client packager according to the choices you make.

- **msi.ini** file - The Windows Installer file is used by the installer to set properties for the client installation. This file is created by the client packager with the following default parameter settings:
  - REBOOT=R

  For more information about msi parameters, see the Endpoint Security Client Management Guide.

- **Initial policy (optional)** - Use an initial policy in your client package to provide a basic level of security for the endpoint computer before it connects to the Endpoint Security server and receives its assigned disconnected policy.

  Unlike the personal policy, the disconnected policy is an enterprise policy, so it cannot be modified by the endpoint user and can be centrally managed by the Endpoint Security server after installation.

  If an endpoint user has both a disconnected and a personal policy, the policies are arbitrated. For more information about these policy types see “Security Policies,” on page 36.

- **userc.C and product.ini** - These files specify VPN settings.

- **cpmsi_tool.exe** - The client packager runs this executable to insert the userc.C and product.ini into the msi database.

- **integrity.pem** - Contains authentication information.

- **updatekeyfiles.xml** - Contains authentication information that the client uses to receive upgrades.
Planning Your Client Distribution

Before beginning to create and deploy your client packages, you should consider the following topics:

- “Deployment Options,” on page 157
- “Client Types,” on page 157
- “New Client Versions,” on page 157
- “Policies,” on page 158
- “VPN Options,” on page 158
- “Installation Options,” on page 163
  - “Install Key (Password),” on page 163
  - “Connection Information,” on page 164
  - “User Identification,” on page 165

Deployment Options

How you distribute your client will depend on the size of the deployment, the experience level of your users, and your available third-party software. This chapter only describes distribution tasks associated directly with the client packager. Before creating your client packages, you should consider the information about the various distribution methods included in the Endpoint Security Client Management Guide.

Client Types

Endpoint Security includes a default client executable for each type of client:

- Flex - This client is intended to be deployed to autonomous users with a degree of familiarity with desktop protection functionality. Flex users would be expected to have the technical knowledge to be responsible for their own firewall configuration. Flex provides the capability for the user to configure the personal policy settings.
- Agent - This client is designed to be configured entirely by an administrator. It has only limited endpoint user interface.

You should choose the type of client to deploy based on your enterprise requirements and endpoint user capabilities. For more detailed information about clients, see the Endpoint Security Client Management Guide. If you have a new version of the Client, you can also import the client into the system so you can include it in policies.

New Client Versions

Check Point sometimes issues new versions of clients. In order to use these new versions in client packages, you must import the installers into the client packager. See “Importing Client Installers,” on page 169.
Policies

It is generally recommended that you immediately establish a basic level of security by including a policy in your policy package. Depending on the type of policy you include, this policy is enforced until either the endpoint user configures a policy, or until the endpoint computer contacts the Endpoint Security and receives the assigned policy.

If you plan to include policies in your client package, it is convenient to create them before you create your package.

You may also want to assign policies to your endpoint users before you distribute clients to them. This is especially highly recommended if you do not include a policy in your package.

For information about creating and assigning policies, see “Managing Security Policies,” on page 46.

VPN Options

You can choose to include Virtual Private Network (VPN) capability with your Agent or Flex client installation package. By providing a secure VPN for your endpoint users, you give them remote access to your network while also administering high levels of privacy and authentication.

This feature combines VPN capability with the security protection of the Endpoint Security client. By using this feature in combination with Enforcement rules, you have the option of controlling access at the VPN gateway based on the presence or absence of certain software. You configure all of this using the Endpoint Security Administrator Console. This VPN functionality is designed to work with the Check Point VPN-1 gateway, so you need the VPN-1 gateway installed on your network before packaging and deploying VPN packages.

This section describes the process of configuring VPN in client packages, and covers the following topics:

- “Migrating from Check Point SecureClient (Optional),” on page 158.
- “VPN Configuration and Package Creation,” on page 160

For information about installing a Check Point VPN-1 gateway, see the Check Point VPN-1 documentation. For more background information about VPN, see the Check Point Virtual Private Networks document, available for download on the Check Point Website.

Migrating from Check Point SecureClient (Optional)

If you previously integrated client and Check Point VPN SecureClient by configuring SCV (Secure Configuration Verification) for the purpose of Cooperative Enforcement, you can now achieve similar goals more easily with Endpoint Security. The VPN feature provides a faster, simplified method of configuring and deploying VPN, and provides end-users with a unified interface for both the client and the VPN. You can still use
client and Check Point SecureClient separately, but doing so does not take advantage of the simplified client management and unified interface.

There are some third-party scripts, which you may have used with SCV, for which there are no Endpoint Security system alternatives. The following third-party scripts are not currently supported in Endpoint Security:

- A script for verifying machine certificates to confirm domain membership
- A script that checks active GPO policies
- A script that blocks USB devices.

See “About Third-Party Scripts,” on page 160 for information about some Endpoint Security alternatives to other types of third-party scripts.

This section describes information and guidance to assist you if you are migrating from Check Point SecureClient.

### Migrating from SCV and Desktop Security Rules

If you previously configured VPN enforcement with Desktop Security rules and SCV, and now want to use the Endpoint Security to configure similar control, the following approach is recommended:

1. Set your Zone Rules (Internet Zone and Trusted Zone) to Low security and by setting Program Control to Allow All.

   This is recommended because it allows you to start with a configuration process that is similar to your prior experience, and helps prevent unexpectedly restrictive experiences for your endpoint users. Later, you can build more complexity into the policy you deploy.

   See “Zone-Based Security,” on page 56 and “Program Control,” on page 69 for information about setting Zone Rules and Program Control.

2. Recreate SCV settings:

   a. Make a note of the endpoint local.scv file (SCV) settings that you want to recreate. (Note that local.scv files are eliminated during endpoint installation of Endpoint Security VPN packages.)

   b. Use Endpoint Security Enforcement rules to recreate the enforcement settings. See “Enforcing Endpoint Security,” on page 97

3. Recreate Desktop Security rules:

   a. Make a note of the inbound and outbound rules in the Desktop Security policy that has been used by your endpoints. These rules are shown in the Desktop Security tab of SmartDashboard.

   b. On Endpoint Security, recreate, as Firewall rules, the inbound and outbound rules that you noted above. See “Managing Firewall Rules,” on page 66 for details.
c. Create a “cleanup” rule: Add a last-precedence Firewall rule, ranked at the bottom of the list, which blocks all traffic. This manually created cleanup rule is necessary because when Zone Rules are set to Low, the hard-coded cleanup rule that blocks all unhandled traffic is disabled.

4. If possible, set the Check Point Desktop Security rules to the following settings in order to ensure that only one firewall driver is active in the system:
   - Source: Any
   - Destination: Any
   - Service: Any
   - Action: Accept

5. Proceed with the steps outlined in “Workflow for Configuring and Deploying VPN in Packages,” on page 162.
   As described in the workflow, be sure to add the Firewall rules and Enforcement rules to the policy assigned to the VPN-1 gateway.

Building a More Advanced Policy
Once you have your basic policy deployed, with a basic level of security for your endpoints, you can begin to create a more advanced policy. For example, you may want to add Program Control to replicate the function of a third-party script that you previously used with SCV. See “Managing Security Policies,” on page 46 for more information.

When you begin to add Program Control and Zone Rules, bear in mind that Program rule permissions and Firewall rules can override Zone rule permissions, as described in “Rule Evaluation and Precedence,” on page 43.

About Third-Party Scripts
While there is no Endpoint Security Enforcement rule that you can use to run a third-party script, you can use Program Control and Enforcement rules to recreate a number of the endpoint checks you may have configured with third-party scripts and SCV. For example:

- You can use Program Control in a disconnected policy to deny network access to peer-to-peer applications.
- You can use Program Control to block access to services like Telnet and FTP.
- You can create Enforcement rules to restrict endpoint network access when endpoints do not have the required antivirus protection.

VPN Configuration and Package Creation
When creating client installation packages with VPN, you can:

- Specify client VPN connection mode (automatic or manual)
- Specify Compact (simplified) or Extended VPN panel views for endpoint users
Configure topology settings, so that the end user does not have to configure a VPN site for initial connection

Configure behavior at the OS (operating system) logon, such as Secure Domain Logon (SDL)

Specify third party authentication, if needed

You also have the option of importing existing VPN configuration files, which may contain configurations other than those listed above, as explained in “Planning Your VPN Configuration,” on page 161.

Creating a VPN client package is similar to basic client installation package creation, but there are some additional required steps. See “Workflow for Configuring and Deploying VPN in Packages,” on page 162.

Planning Your VPN Configuration

To prepare for creating a VPN client package, select a VPN configuration method and decide which VPN settings you want.

To prepare for creating a VPN client package:

1. Determine which of following methods you will use:

   • **Configure VPN settings while creating the client package.** Use this method if you want to be able to create and edit the client package VPN settings using the Endpoint Security Administrator Console.
     
     Once you create a VPN package with the Administrator Console settings (rather than by importing files), you can easily:
     
     • Make new packages by copying the package.
     • Edit the configuration with the Client Packager.

   • **Import existing VPN configuration files.** Use this method if there is an existing VPN configuration, created prior to the existence of VPN settings in the client packager, that you want to replicate and deploy. (Note that once you import configuration files, you are not able to use the Administrator Console to edit those settings.)
     
     While creating the client package, you import existing VPN settings by specifying the location of product.ini and userc.C files for the settings you want. The product.ini and userc.C files are VPN configuration files.
     
     The most recent default installation locations of these two files on endpoint computers are:
     
     <Client Inst>|SecuRemote|database|userc.C
     <Client Inst>|SecuRemote|product.ini
     
     To prepare for configuration, make sure the product.ini and userc.C files are in an accessible location (local or via network) so that you can select them during configuration. For more information about product.ini and userc.C files, see the Check Point Virtual Private Networks document, available for download at the Check Point Website.
2. Determine which VPN configuration settings are most suitable for your environment.
   
   This step includes deciding which policies you want the VPN gateway to use. For example, you may want to provide VPN users with stricter security policies.

3. Decide whether or not to control endpoint computer access, based on the presence or absence of certain software, at the VPN gateway level.

   Enforcement rules can require or prohibit specified programs, files, antivirus software, and other conditions on the endpoint computer before allowing unrestricted network access. When Enforcement rules are in the policy assigned to the VPN gateway, endpoint VPN access is controlled according to those rules. If you wish to establish this access control at the VPN gateway level, you will need to ensure that Enforcement rules are added to the policy being used by the VPN gateway. See the chapter on “Enforcing Endpoint Security,” on page 97.

   If you previously integrated the Endpoint Security client and SecureClient by configuring a local .scv file (Secure Configuration Verification) for cooperative enforcement, see “Migrating from SCV and Desktop Security Rules,” on page 159.

Workflow for Configuring and Deploying VPN in Packages

The process for including VPN in client installation packages consists of the following steps.

1. Plan your VPN configuration if you have not already done so.
   
   See “Planning Your VPN Configuration,” on page 161.

2. Create a policy to include in the client package (optional).
   
   Including a policy in a package is beneficial because it ensures a basic level of security until the endpoint user configures a policy or receives the assigned policy from the Endpoint Security server. See “Policies,” on page 158 for more information.

   A Default VPN Policy, designed to keep out any incoming traffic that is not encrypted, is included for your convenience. See “Using a Default VPN Policy,” on page 53 for information on how to access and configure it.

3. Configure the VPN-1 gateway within Endpoint Security.
   
   a. Add the gateway to your Endpoint Security. See “Adding Gateway Catalogs,” on page 152. This step allows the Endpoint Security server to communicate with the VPN gateway.

   b. Assign policies to the gateway (optional).
      
      If you prefer to assign a specific policy to this gateway, you can do so now. If you do not assign a specific policy, the inherited policy is used by the gateway.
4. Add any Firewall rules, Enforcement rules, and Program Rules to the policy assigned to the VPN-1 gateway. (optional).

This step is necessary only if you want to control access, based on endpoint software checks, at the VPN gateway level.


5. Create the client package.

- Choose VPN Agent or VPN Flex from the New Package menu.
- Use the VPN Settings tab to configure VPN settings for the package (optional).
  As discussed in “Planning Your VPN Configuration,” on page 161, you can do either of the following:
  - Configure VPN settings using the settings provided in the packager.
  - Or, import existing VPN settings from a product.ini file and userc.C file.
    Use the browse dialog provided to locate and select the files.
- Complete your configuration of the client package.
  For more information about settings, see the online help and “Creating Client Packages,” on page 167.

6. Deploy the client package.

See “Distributing Packages,” on page 167.

Installation Options

When planning your client packages, consider the following installation options:

- “Install Key (Password),” on page 163
- “Connection Information,” on page 164
- “User Identification,” on page 165
- “Custom Parameters,” on page 165

Install Key (Password)

The install key is a password needed in order to uninstall or upgrade the client. A default install key is created if you do not set one. The install password does the following:

- Prevents endpoint user changes to the installation
  Preventing endpoint users from uninstalling the client is important for the security of your network. See “Prevention of Client Uninstalls,” on page 164.
- Allows administrators to perform silent upgrades and uninstalls
  See “Silent installations and upgrades,” on page 164.
- Prevents endpoint users from blocking administrator-initiated upgrades and uninstalls with the user password. The install key overrides the user password. For more information about user passwords, see the Endpoint Security Client Management Guide.

**Default Install Key**

As a back-up safety mechanism to protect your network from endpoint computers that are not protected by an Endpoint Security client, a default install key is created if you do not create one. This key prevents endpoint users from uninstalling the client because it is required in order to uninstall or upgrade the client.

If you do not set an install key when creating the client installation package, the default key is generated. The default install key is `secret`.

Create your own install key while creating the client package, on the Package Details page. For navigation information, see “Package Details,” on page 193.

**Prevention of Client Uninstalls**

The install key prevents endpoint users from uninstalling the client. This key will be required for any subsequent changes to the installation.

It is highly recommended that you create a unique install key (rather than use the default key) in client installation packages. This prevents endpoint users from guessing the key and uninstalling the client. Allowing endpoint computers that are not protected by an client to connect to your network is a security risk.

If you do not set a unique install key and are using a supported gateway, it is highly recommended that you use the gateway to restrict or terminate the connection if the client is not running. This prevents the endpoint user from removing the client and then connecting to your network while unprotected. See the Endpoint Security Administrator guide for more information about cooperative enforcement with supported gateways.

**Silent installations and upgrades**

Because there is always an install key (the default one or your custom one), you upgrade or uninstall the client without any user interaction. On the endpoint, the client icon appears in the desktop system tray during the upgrade or installation, but no action is required of the user.

Note that without an install key, the TrueVector security software (low level software that monitors Internet activity) cannot validate the request to shutdown. This would result dialog asking the user for permission to continue.

**Connection Information**

It is essential that the clients have the connection information they need to contact the Endpoint Security server. The necessary connection information for the Endpoint...
Security server is provided by default. You can also manually change this information or import configuration files (config.xml) from another server.

If you change the connection information for your Endpoint Security server, you must distribute new package files with the new server's connection information.

**User Identification**

You can also assign a Single Sign On ID or a User ID to your endpoint computers as part of the client package.

A Single Sign On ID allows endpoint users to sign on once per start up.

A User ID allows you to add users to custom catalogs by that name. If you want to include the endpoint computers that receive this package in a custom catalog, type the catalog name and, optionally, the group name in the **User ID** field.

Use the following format: `manual://<Catalog_Name>/<Group_Name>`

When the endpoint computers that receive this package connect to the Endpoint Security server, they will become members of the catalog and group you specified here.

If you are creating a client package to use with the auto-upgrade feature (and if you are using a different Endpoint Security server than you used for the initial deployment) and you want to view installation results in the auto-upgrade report, then you must use the same user ID (connection string) for the upgraded client package as you used for the initial client deployment.

**Custom Parameters**

A **Custom Parameter** field is included in the Advanced Settings of the client packager. In this field you can enter commands to further refine installer behavior. Refer to the client parameters described in the *Endpoint Security Client Management Guide* for detailed information on the commands and values you can use.

To enter custom parameters, use the `<parameter>=<value>` format, and to specify multiple custom parameters separate each with a space.

For example:

```
RESETVPNCONFIG=YES FORCEREROOTDIALOG=YES
```
Client Package Workflow

Use the following workflow to distribute client packages to your endpoint computers.

1. Plan your distribution.
   If you have not already done so, familiarize yourself with your distribution options. You should be familiar with both the information in “Planning Your Client Distribution,” on page 157 and the various possible distribution methods detailed in the Endpoint Security Client Management Guide.

2. Create your policies (optional).
   If you plan to include policies in your client package, it is more convenient to create them before you create your package. For more information about creating policies, see “Managing Security Policies,” on page 46.

3. Import new client installers (optional).
   If you have received a new version of the clients, you will need to import the installers into the client packager. See “Managing Client Installer Versions,” on page 169.

4. Create the package.
   See “Creating Client Packages,” on page 167.

5. Distribute packages.
   Use the distribution method of your choice to deliver packages to the endpoint users. See “Distributing Packages,” on page 167.
Managing Client Packages

This section includes the following topics:

- “Creating Client Packages,” on page 167
- “Distributing Packages,” on page 167
- “Automatically Upgrading Clients,” on page 169
- “Managing Client Installer Versions,” on page 169

Creating Client Packages

Create client packages to bundle client executables with configuration information and policies.

To create a client package:

1. Go to the Client Configuration page.
   For navigation information, see “Client Configuration,” on page 191.
2. Click New Package and choose your client executable option.
3. Configure your package options.
   For more information about these options, see the online help.
   a. In the Package Details page, configure your installation options.
      The Endpoint Security server can communicate with all 6.x versions of the clients, but it is recommended that you use the same version as your Endpoint Security server or higher. Using the same version ensures that all features will perform as expected.
   b. If you have enabled VPN in this package, click VPN Settings and enter your VPN information.
   c. If you want to specify connection and user ID settings other than the default, click Advanced Settings.
4. Click Save.

Distributing Packages

You can distribute a client package using any of the following methods:

- Exporting Client Packages - You can export the client package and distribute it to the endpoint user using your own distribution method. See “Exporting Client Packages,” on page 168.
Distributing a Client Package URL - You can distribute a link that directs the endpoint user to a page that includes the client package. See “Distributing the Client Package URL,” on page 169.

Exporting Client Packages

You can export a client package as an executable .exe file.

For Group Policy Object (GPO) and third-party deployments, you can then use a command-line tool to convert the package into an MSI (Microsoft Installer) file.

To export a client package .exe file:

1. Go to the Client Configuration page.
   For navigation information, see “Client Configuration,” on page 191.
2. Click Export.
3. Browse to the location where you want to save the client package and click Save.
   Do not click the Open button as the executable will install on the administrator's console machine.

You can now use whichever distribution method you choose to distribute the Endpoint Security client package to your endpoint users.

To convert the client package .exe file to an MSI file:

1. Go to the directory to which you saved the .exe file.
   Example:
   `cd c:\downloads`
2. Run the .exe package installer with the parameter msi.
   For example:
   `<client package filename>.exe msi`
   The directory now contains a new file called `<client package filename>.msi`, which you can use to perform GPO or third-party deployments of the client.

Refer to the Client Management Guide for more information about GPO and third-party deployments.
Distributing the Client Package URL

To distribute a URL to download the client

1. Go to the Client Configuration page.
   
   For navigation information, see "Client Configuration," on page 191.

2. Click the client package name that you wish to distribute.

3. Copy the Package Download URL.

4. Distribute the URL to endpoint users using e-mail or your intranet:
   - E-mail the full path of the client package to endpoint users. Users can simply click on the hyperlink provided or copy and paste the URL into a browser address field.
   - Post the download URL to your intranet as a convenient method of software distribution.

Both of the above methods rely on the endpoint user's cooperation. However, once clients are installed, upgrades can be handled seamlessly by way of policy enforcement and auto-upgrade.

Automatically Upgrading Clients

You can upgrade endpoint clients automatically by creating a client enforcement rule and referring to the location of the upgraded client package. The enforcement rule sets the minimum client version allowed on an endpoint computer. You can set the remediation options to automatically upgrade the client with the endpoint user's confirmation, or prompt endpoint users to upgrade.

For more information about creating client rules and using auto remediation see "Client Enforcement Rules," on page 112.

Managing Client Installer Versions

The Client Packager page lists all the clients that were installed with your Endpoint Security server. If you need to package another version of the client, you will need to import it.

Importing Client Installers

Importing a client makes it available for inclusion in client packages. When you import a client .msi file, you get both Flex and Agent in one file.

To import client installers:

1. Save the new client installers to the same host as the Endpoint Security server.
2. Go to the Client Configuration page.
   For navigation information, see “Client Configuration,” on page 191.

3. Click Manage Installer Versions.

4. Click New.

5. Click Browse and select the .msi file for the new client installer.

6. Complete the other fields on this page for the client installer.
   Be sure to use the correct version number and language.

7. Click Import.

**Deleting Client Installers**

If you want to prevent other administrators from distributing older versions of the clients

**To delete client installers:**

1. Go to the Client Configuration page.
   For navigation information, see “Client Configuration,” on page 191.

2. Click Manage Installer Versions.

3. In the row for the installer, click Delete.
   If you are currently using this installer in any client packages, you will not see the delete option. You must remove the installer from all the client packages.
Monitoring

Use the reports to monitor the status of your clients.

**Client Connectivity Report**

The Client Connectivity Report gives an up-to-date overview of connected and unconnected clients. Connected clients are organized according to how long they have been connected. The report keeps you up to date on connectivity issues, such as when an unusual number of endpoints are unconnected during working hours.

A client is connected when the endpoint computer is turned on, the user is logged in and the client can contact the Endpoint Security server. It is therefore normal for a majority of endpoints to be unconnected during non-working hours, when most users have turned their computers off.

For navigation information for this report, see “Client Connectivity Report,” on page 171.

**Client Version Report**

The Client Version Report shows which client versions are running on your network and which endpoints are running them. Use the report when you have deployed a new client package and want to confirm that endpoints are running the new client.

For navigation information for this report, see “Client Version Report,” on page 171.
Chapter 20
Monitoring Client Security

In This Chapter

Setting Log Upload Parameters page 173
Reports page 173

Endpoint Security provides a variety of reports for monitoring security on your endpoints. Reports show whether your endpoints comply with client and policy requirements, enforcement rules, firewall rules, regular spyware scans, and antivirus software requirements. They also provide information about endpoint security events, such as prohibited program activity and prohibited file transfers over e-mail. If a user is unknown, reports provide user connection information instead of a catalog name. Reports present overviews of general security trends as well as detailed information about individual endpoints.

You can drill down through some Endpoint Security reports to detailed reports in the reporting tool, SmartPortal. Even if you have installed Endpoint Security in standalone mode, you still have the necessary components of Check Point SmartCenter to allow this access to the related SmartPortal reports. You do not need to explicitly choose to install SmartPortal to use this reporting function. You can also access these reports through SmartTracker, if you have installed it.
Setting Log Upload Parameters

Endpoint Security bases its reports on logs uploaded from clients. Log upload parameters have default values, but you can change the defaults to control how often clients send the logs.

To set log upload parameters:

1. Go to the Client Configuration page.
   For navigation information, see “Client Configuration,” on page 191.
   If you have not already configured client settings, the defaults are displayed.
2. Click Edit.
3. Complete the fields in the Log Upload and Log Upload Size areas to configure the parameters.
   See the online help for more information about completing these fields.

Setting excessively low parameters can result in a loss of performance. Setting excessively high parameters will result in your reports being less up-to-date.

Reports

Reports are discussed in detail in the context of their related features. Endpoint Security includes the following reports:

- **Endpoint Monitor Reports:**
  - Endpoint Status Report
    See “Viewing Compliance Status,” on page 119.
  - Client Connectivity Report
  - Client Version Report
  - Policy Assignment Report
  - Enforcement Violations by Rule
    See “Violations by Rule and Policy,” on page 120.
  - Enforcement Violations by Policy
    See “Violations by Rule and Policy,” on page 120.
  - Antivirus Provider Brands Report
    See “Viewing Antivirus Versions,” on page 120.
- **Check Point Antivirus Scanned Date Report**
  See “Monitoring Infection Scan and DAT Update Status,” on page 140.

- **Check Point Spyware Scanned Date Report**
  See “Monitoring Infection Scan and DAT Update Status,” on page 140.

- **Check Point Disk Protection**
  Reports on Pointsec for PC 5.0 and higher.

- **Check Point Port Protection**
  Reports on Pointsec Protector 4.8 and higher.

- **Endpoints Report**
  See “Configuring a Test Group,” on page 137.

- **Infection History Reports**
  See “Monitoring Spyware and Virus Event History,” on page 140.

If an endpoint has no activity for 28 days, it is not shown in the reports.
In This Chapter

Managing Your Products       page 177
Managing Communication       page 183

Use this chapter to perform general configuration and maintenance tasks for your Endpoint Security system. Most of the tasks in this chapter are optional, depending on your other configuration choices.
Managing Your Products

This section contains the following topics:

- “Licensing,” on page 177
- “Version Information,” on page 179
- “Starting and Stopping Endpoint Security,” on page 179
- “Uninstalling Endpoint Security and other Check Point products,” on page 180

Licensing

Use the instructions in this section to manage your licenses for Endpoint Security and its features. This section contains the following topics:

- “Introduction to Licensing,” on page 177
- “Expired or Exceeded Licenses,” on page 178
- “Licensing Workflow,” on page 178
- “Generating Licenses,” on page 179
- “Attaching Licenses,” on page 179

Introduction to Licensing

All installations require a client license, which allows you to run clients on your endpoints. Optionally, you can also purchase licenses for special Endpoint Security features. The following licenses are available for Endpoint Security:

- **Clients**—Permits a specified number of endpoints to run the client. This license is required.
- **Smart Defense Program Advisor**—Permits Endpoint Security to receive the latest Program Advisor updates. The license is good for an unlimited number of endpoints.
- **Check Point Antispyware (endpoints)**—Permits a specified number of endpoints to use Check Point Antispyware.
- **Check Point Antispyware (updates)**—Permits the Endpoint Security server to receive the latest Antispyware updates.
- **Check Point Antivirus (endpoints)**—Permits a specified number of endpoints to use Check Point Antivirus.
- **Smart Defense Antivirus (updates)**—Permits Endpoint Security to receive the latest Antivirus updates.

You can obtain these licenses from the Check Point User center or from your Check Point representative.
You must install and attach Endpoint Security licenses with one of the Check Point license management tools: SmartUpdate, the cplic command, or (for local licenses only) the Check Point Configuration Tool. (For information on these options, see “Attaching Licenses,” on page 179.)

After a feature has been enabled on the Endpoint Security server, you can incorporate that feature into security policies, which you can then deploy to clients. An endpoint computer's active policy controls which features are enabled on that endpoint.

**Expired or Exceeded Licenses**

Each Check Point product comes with a trial license that allows unrestricted use of the product for 15 days. Trial licenses include all product features.

For complete details on all licensing options and enforcement behaviors, contact your Check Point representative.

For the Endpoint Security clients license, the Endpoint Security server checks for the maximum number of endpoints that connected during the last 24 hours. This check runs every 24 hours after the server starts. If your installation exceeds the number of allowed endpoints, the Endpoint Security server goes into read-only mode. Your endpoints are still protected by their existing policies, but you will be unable to make changes until you enter your new license through Smart Update. Contact your Check Point representative to get a new license and restore editing privileges.

While you are waiting for your new Endpoint Security clients license, you can use a trial license. Contact your Check Point representative to obtain a trial license.

If a feature license expires, Endpoint Security either disables editing privileges or prohibits administrator access to the feature.

**Licensing Workflow**

When licensing your products, decide whether to manage the licenses centrally or locally. The differences between central and local licensing are as follows:

- **Central licensing**—You use SmartUpdate or the cplic command to store licenses in a central repository on SmartCenter Server, and then to attach the licenses to the desired computers. Central licenses are not tied to an IP address, and therefore can be reassigned as necessary. This is the recommended form of license management, and it is especially useful for distributed installations.

- **Local licensing**—Each license is tied to the IP address of the computer on which it is installed. Licenses are attached either with SmartUpdate or (locally) with the Check Point Configuration Tool or the command-line interface. If the IP address of the licensed computer changes, you must generate a new license for that computer.

**To license your products:**

1. Generate the licenses.
   
   See “Generating Licenses,” on page 179.
2. Attach the licenses.

See “Attaching Licenses,” on page 179.

Generating Licenses

Check Point provides certificate keys for each license you purchase. Use the certificate keys to generate licenses.

To generate a license:

1. Gather the following information:
   - Certificate key
   - Host IP address (For central licenses, use the SmartCenter Server host IP address.)
2. Log in to the Check Point User Center (www.checkpoint.com/usercenter) and navigate to the Getting Started page.
3. Follow the User Center instructions for generating a license.

Attaching Licenses

Use SmartUpdate or the cplic command-line tool to attach licenses to your installations. You must use one of these methods, even if you have installed Endpoint Security as a standalone product.

For instructions on using SmartUpdate to attach the license, see the SmartCenter User Guide. For information on cplic, see the Check Point Command Line Interface Guide. You can also use the Check Point Configuration Tool to attach licenses locally. For information on the configuration tool, see the Check Point Getting Started Guide, and the configuration tool's online help.

Version Information

It is important to know the version of your Endpoint Security server. This helps you to make sure you are using the correct documentation, the correct versions of the Endpoint Security clients, and is useful if you need to contact support.

To view your version information:

1. Click About.

Starting and Stopping Endpoint Security

This section explains how to manually start, stop, and restart the Endpoint Security server and the Apache httpd server.

Use the instructions appropriate to your operating system:
Use the Control Panel to start, stop, or reset the Endpoint Security, Apache, or Tomcat services.

**To stop, start, or reset the services**

2. Right-click on the service and choose the option you want.

**Linux**

This section explains how to start and stop Endpoint Security.

**To start or stop Endpoint Security:**

1. Log in to Endpoint Security host as root.
   
   ![root@localhost /]

2. Run the start, stop, or restart shell:
   
   - **Start:** `<Install Directory>/bin/IntegrityStart`
   - **Stop:** `<Install Directory>/bin/IntegrityStop`

   The default install directory is `/opt/CPIntegrity`

---

**Uninstalling Endpoint Security and other Check Point products**

This section explains how to uninstall Endpoint Security and other Check Point products. Refer to the instructions appropriate for your operating system:

- “Windows,” on page 180
- “Linux,” on page 181
- “Check Point SecurePlatform,” on page 181

**Windows**

To uninstall on Windows:

1. Go to Start | Control Panel | Add or Remove Programs and remove Endpoint Security.
2. On the same computer, remove the Check Point software packages, making sure to remove the Check Point VPN-1 Pro component last, after removing all other Check Point software components.

3. If you have a distributed installation, access the SmartCenter host and go to the command line. Stop all Check Point services by running `cpstop`. Then go to Start | Control Panel | Add or Remove Programs. Remove the Check Point software packages, making sure to remove the Check Point VPN-1 Pro component last. Repeat this step for any other SmartCenter hosts in your configuration (for example, a separate host running a remote log server).

**Linux**

Follow the instructions below to uninstall Check Point software from a Linux system. On any host from which you are removing Check Point software, you must remove the `CFSuite-xxx-00` component (where `xxx` is the version number) last, after removing all other Check Point software components.

**To uninstall from a Linux system:**

1. Navigate to the uninstallation directory (by default, `/opt/CPIntegrity/Uninstall_Integrity`), and issue the following command:
   ```bash
   ./Uninstall_Integrity
   ```
   At the prompt, press `Enter`. The Endpoint Security uninstallation wizard starts.

2. Work through the uninstallation wizard.

3. Issue the following command to see a list of Check Point components installed on your system:
   ```bash
   rpm -qa | grep CP
   ```
   Note that this command displays all software components containing “CP,” including some which are not Check Point components.

4. Issue the following command for each component to remove, making sure to remove the `CFSuite-xxx-00` component (where `xxx` is the version number) last.
   ```bash
   rpm -e <package_name>
   ```

5. If you have a distributed installation, access the SmartCenter host and run `cpstop`. Then repeat steps 3 and 4 on the SmartCenter host.
   Repeat this step for any other SmartCenter hosts in your configuration (for example, a host running a remote log server).

**Check Point SecurePlatform**

There is usually no reason to uninstall a Check Point product from a SecurePlatform host while leaving SecurePlatform intact. If you want to install a newer version of a Check Point product on SecurePlatform, it is recommended to back up your data and then reboot the host from the installation CD. Rebooting from the CD will remove
SecurePlatform from the host and replace it with the version appropriate for your new installation. (Installation CDs for the SecurePlatform versions of Check Point products include the appropriate version of SecurePlatform for the installation.)

In rare cases, you may want to uninstall a Check Point product while leaving SecurePlatform intact. For example, if you are currently running Endpoint Security and SmartCenter on one host, and you want to convert to a distributed installation (with Endpoint Security and SmartCenter on separate hosts), you would back up your data and then uninstall Endpoint Security or SmartCenter from the current host (without uninstalling SecurePlatform). In such cases, follow the instructions below.

To uninstall from a SecurePlatform system:

1. On the desired computer, stop all Check Point services by running `cpstop`.
2. To uninstall Endpoint Security, navigate to the uninstallation directory (by default, `/opt/CPIntegrity/Uninstall_Integrity`), and issue the following command:
   ```
   ./Uninstall_Integrity
   ```
   At the prompt, press `Enter`. The Endpoint Security uninstallation wizard starts.
3. Work through the uninstallation wizard.
   Remove Endpoint Security.
   If you are removing only Endpoint Security, this step completes the process.
4. Run the following command to see a list of Check Point components installed on your system:
   ```
   rpm -qa| grep CP
   ```
   Note that this command displays all software components containing “CP,” including some which are not Check Point components.
5. Run the following command for each component to remove, making sure to remove the `CPSuite-xxx-00` component (where `xxx` is the version number) last:
   ```
   rpm -e <package_name>
   ```
   You must remove Endpoint Security before removing SmartCenter.
Managing Communication

Use the instructions in this system to manage communication between the Endpoint Security server, the Endpoint Security clients, other Check Point products, and the Internet.

This section contains the following topics:

- “Allowing Endpoint Hotspot Registration,” on page 183
- “Proxy Configuration,” on page 184
- “Configuring a RADIUS Server,” on page 186
- “Changing your JDBC IP Address,” on page 188
- “Client Logging,” on page 189

Allowing Endpoint Hotspot Registration

Some policies are too restrictive to allow wireless hotspot use for users who want to access your network from a hotel or public place. This is especially relevant for disconnected policies, and for enterprise policies that are enforced when disconnected, because these policies are in effect when a user is trying to connect to a wireless hotspot.

For this reason, the Enable Hotspot Registration feature makes temporary access possible, while maximizing security by controlling the parameters of hotspot-specific port openings. Regardless of the restrictiveness of a policy, you can allow a temporary, controlled opening by selecting the Enable Hotspot Registration option in the policy.

If you do not enable Hotspot Registration, and the client policy doesn’t allow access to hotspot ports, users will not be able to access the wireless hotspot Web page, and therefore they will not be able to access the Internet or your network.

Hotspot Registration works with most VPN types and configurations.

How Hotspot Registration Works on the Endpoint

When the endpoint user is at a public space or hotel, they access your network through the following process:

1. The user selects Register to Hotspot/Hotel from the Endpoint Security icon in their system tray menu.
2. The three ports common to Internet hotspot registration (80, 8080, 443) are opened. A maximum of five IP addresses are allowed during the connection time.
3. The Hotspot port opening lasts until any of the following occurs:
   - The user connects to the network
   - Ten minutes pass
   - Three failed connection attempts
To enable hotspot registration in a security policy:
1. Go to the Client Settings page.
   For navigation information, see “Client Settings,” on page 191.
2. Select the Enable Hotspot Registration option.
3. Click Save.

Proxy Configuration

If you plan to use the Program Advisor feature, Antispyware, or Antivirus features in an environment that includes a proxy server for Internet access, perform the configuration steps below to let Endpoint Security connect to Check Point's central servers (containing Program Advisor settings or Antispyware/Antivirus definitions) through the proxy server. Note that all configuration entries are case-sensitive.

You can perform these steps at any time after installation. If desired, you can perform these steps when enabling Program Advisor, Antispyware or Antivirus.

Configuration steps are provided for the following operating systems:
- “Windows,” on page 184
- “Linux,” on page 185

Windows

To configure a proxy server:
1. Open the Registry Editor (regedit.exe).
2. Edit “My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0 \IntegrityTomcat\Parameters\Java\options” by adding the following:
   ```
   -DproxySet=true
   -Dhttp.proxyHost=<hostname>
   -Dhttp.proxyPort=port
   -Dhttps.proxyHost=<hostname>
   -Dhttps.proxyPort=port
   ```
3. Close the Registry Editor.
4. Open the Services panel.
5. Stop the "Check Point Tomcat" service, and then restart it.

If you are using Program Advisor, you must configure outbound internet connectivity to both of these locations:

- PA2.zonelabs.com
- cm2.zonelabs.com

If you have configured offline updates, you must allow traffic to and from the appropriate updates server:

- Antivirus update server - http://kav-integrity.zonelabs.com/

Refer to your device instructions for information about how to configure this access.

**Linux**

Follow the procedure that is appropriate for your installation.

**To configure a proxy server (in a standard installation):**

1. Edit `~/engine/bin/catalina.sh`, replacing the line:
   ```bash
   JAVA_OPTS=-Xms256M -Xmx512M -Djava.awt.headless=true
   ```
   with the line:
   ```bash
   JAVA_OPTS=-Xms256M -Xmx512M -Djava.awt.headless=true -DproxyHost=true -Dhttp.proxyHost=hostname -Dhttp.proxyPort=port -Dhttps.proxyHost=hostname -Dhttps.proxyPort=port
   ```

2. Save the file.
3. Restart Endpoint Security by issuing:
   ```bash
   <Install Directory>/bin/IntegrityStop
   <Install Directory>/bin/IntegrityStart
   ```
   The default install directory is `/opt/CPIntegrity`

**To reset the JAVA_OPTS environment variable:**

1. Use the appropriate `setenv` call to reset the value of JAVA_OPTS to:
   ```bash
   "-Xms256M -Xmx512M -Djava.awt.headless=true -DproxyHost=true -Dhttp.proxyHost=hostname -Dhttp.proxyPort=port -Dhttps.proxyHost=hostname -Dhttps.proxyPort=port"
   ```
Configuring a RADIUS Server

The Endpoint Security server is configured by default to use its own administrator authentication method. If you wish to use a RADIUS server instead, you will need to configure it.

Prerequisites

Before beginning to configure your RADIUS server, make sure you have done the following:

- Record the RADIUS server host name or IP address and port (default port is 1812).
- Record your RADIUS server shared secret.
- Create an Endpoint Security account, called “masteradmin” on the RADIUS server.

Workflow

To configure the RADIUS server:

Perform the following steps to configure the RADIUS server. Configuration consists of updating a configuration file and a properties file.

1. Update the configuration file.
   - See “Updating the configuration file,” on page 187.

2. Configure the properties file.
   - See “Configuring the properties file,” on page 187.

If you are using Program Advisor, you must configure outbound internet connectivity to both of these locations:

- PA2.zonelabs.com
- cm2.zonelabs.com

If you have configured offline updates, you must allow traffic to the appropriate updates server:

- Antivirus update server - http://kav-integrity.zonelabs.com/

Refer to your device instructions for information about how to configure this access.
**Updating the configuration file**

To update the configuration file:
1. Shutdown the Endpoint Security server.
2. Log in.
   - SPLAT users should log in as ‘admin’. Windows users should log in as an administrator.
3. Go to the configuration file location.
   - For Windows the default location is: `<ENDPOINT_SECURITY_USER_INSTALL_DIR>/engine/webapps/ROOT/conf`
   - For Linux the default location is: `<ENDPOINT_SECURITY_USER_INSTALL_DIR>/engine/webapps/ROOT/conf`
4. Create a backup of integrity.xml.
5. Open template-integrity-config.xml in a text editor.
6. In the AdminConsole node, remove the comment tags from the first RADIUS JAAS node, and remove the JAAS node for ‘inbuilt authentication of admin users’.
7. Save your changes and close the file.
   - Make sure your XML is well-formed.

**Configuring the properties file**

To configure the properties file:
1. Go to the location of the properties file.
   - For Windows, the default location is: `<ENDPOINT_SECURITY_USER_INSTALL_DIR>/engine/webapps/ROOT/conf`
   - For Linux, the default location is: `<ENDPOINT_SECURITY_USER_INSTALL_DIR>/engine/webapps/ROOT/conf`
2. Create a backup of integrity.global.properties.
3. Open install-upgrade.properties in a text editor.
4. Specify the following properties:
   - `radius.authtype=<CHAP or PAP>`
   - `radius.server=<IP address of your radius server>`
   - If your RADIUS server is on the same computer as Endpoint Security, you must log in using the IP address rather than “localhost.” To do this, open a browser...
and use the IP address (instead of the string "localhost") to access the Endpoint Security login page.

- radius.port=<Port for your radius server. Usually 1812.>
- Radius.secret=<Radius secret code>
- upgrade.from.version=<empty>

5. Save your changes and close the file.

6. Go to the utility location.

   For Windows, the location is:
   
   %ProgramFiles%\CheckPoint\Integrity\engine\webapps\ROOT\bin
   
   For Linux, the directory is:
   
   /opt/CPIntegrity/engine/webapps/ROOT/bin

7. Run the upgrade utility appropriate for your operating system:

   - upgradeServer.bat (Windows)
   - upgradeServer.sh (Linux).

   If you are migrating from Integrity 5.x do not run these utilities until you have logged into the Endpoint Security server to complete the migration.


### Changing your JDBC IP Address

When you install your Endpoint Security server, it uses the startup.xml file to locate the database and get the configuration properties. If you set an IP address instead of a hostname for your database and later change your database location, Endpoint Security will not be able to connect to the database until you reset the IP.

#### To reset the IP Address:

1. Change the /conf/startup.xml to point to the new database IP.
2. Change the JDBC IP in the CONFIG_PROPERTY table in the Database.

   The properties to change are:

   - db.main.URL
3. Restart the server.

**Client Logging**

Use the client logs to troubleshoot issues with your clients. Your endpoint users can use the Client Diagnostic Utility to gather the most commonly-needed logs. Your endpoint users will need to have permissions to modify registry keys.

**To log client events:**
1. On the endpoint computer, go to the C:\program files\checkpoint\Integrity Client folder.
2. Double click the TVDEBUG.REG file and allow it to add information to the registry. This enables debug logging.
3. Reboot to have the settings take effect.
4. Have the endpoint user recreate the problem and note the time that it occurred.
   The endpoint user can now use the log upload utility to gather the relevant logs into one file.

**To gather logs:**
1. On the endpoint computer, go to C:\program files\checkpoint\Integrity Client. Double click the Client Diagnostic Utility file.
2. Optionally, you can change the **File Destination**.
   The utility will place the logs in a zip file at the destination you specified. When you have finished debugging the issue, you should deactivate the debug logging.

**To deactivate debug logging:**
1. On the endpoint computer, go to the C:\program files\checkpoint\Integrity Client folder.
2. Double click the TVDEBUG.REG file and allow it to add information to the registry. This disables debug logging.
3. Reboot to have the settings take effect.
Appendix

Administrator Console Navigation

This appendix gives navigation paths for Endpoint Security Administrator Console pages.

Administrator Console Navigation Reference

Use the following table to locate pages in the Administrator Console. Where there is a version of the page for a new item and a version for editing an existing item the navigation for both is given. Depending on your administrator role and permissions, you may be only able to view some pages.

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Check Point Endpoint Security</td>
<td>About</td>
</tr>
<tr>
<td>Access Zones</td>
<td>Policies</td>
</tr>
<tr>
<td>Add Enforcement Rules</td>
<td>Policies</td>
</tr>
<tr>
<td>Add Firewall Rule to Policy</td>
<td>Policies</td>
</tr>
<tr>
<td>Add Locations to Zone</td>
<td>Policies</td>
</tr>
<tr>
<td>Add Program Rules</td>
<td>Policies</td>
</tr>
<tr>
<td>Add Restriction Firewall Rules to Policy</td>
<td>Policies</td>
</tr>
<tr>
<td>Administrator</td>
<td>Administrators</td>
</tr>
<tr>
<td></td>
<td>Administrators</td>
</tr>
<tr>
<td>Page Name</td>
<td>Location</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Administrator Manager</td>
<td>Administrators</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>Client Configuration</td>
</tr>
<tr>
<td>Anti Virus/AntiSpyware</td>
<td>Policies</td>
</tr>
<tr>
<td>Antivirus Provider Brands Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Antivirus Reference Clients</td>
<td>System Configuration</td>
</tr>
<tr>
<td>Antivirus Rule</td>
<td>Policies</td>
</tr>
<tr>
<td>Change Password</td>
<td>Change Password</td>
</tr>
<tr>
<td>Check Point Antivirus Scanned Date Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Check Point Spyware Scanned Date Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Client Configuration</td>
<td>Client Configuration</td>
</tr>
<tr>
<td>Client Connectivity Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Client Package Installer Versions</td>
<td>Client Configuration</td>
</tr>
<tr>
<td>Client Rule</td>
<td>Policies</td>
</tr>
<tr>
<td>Client Settings</td>
<td>Policies</td>
</tr>
<tr>
<td>Client Updates</td>
<td>Home</td>
</tr>
<tr>
<td>Client Version Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Custom Catalog</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Custom Group</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Page Name</td>
<td>Location</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Endpoint Details</td>
<td>Endpoint Activity I Apply Filter</td>
</tr>
<tr>
<td>Endpoint Manager</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Endpoint Status Report</td>
<td>Endpoint Monitor I &lt;choose report&gt;</td>
</tr>
<tr>
<td>Endpoints Report</td>
<td>Endpoint Activity</td>
</tr>
<tr>
<td>Enforcement Rules Manager</td>
<td>Policies I Manage Policy Objects I Enforcement Rules</td>
</tr>
<tr>
<td>Enforcement Settings</td>
<td>Policies I Edit I Enforcement Settings</td>
</tr>
<tr>
<td>Enforcement Violations by Policy</td>
<td>Endpoint Monitor I &lt;choose report&gt;</td>
</tr>
<tr>
<td>Enforcement Violations by Rule</td>
<td>Endpoint Monitor I &lt;choose report&gt;</td>
</tr>
<tr>
<td>Firewall Rule Manager</td>
<td>Policies I Managing Policy Objects I Firewall Rules</td>
</tr>
<tr>
<td>Firewall Settings</td>
<td>Policies I Edit I Firewall Settings</td>
</tr>
<tr>
<td>Gateway</td>
<td>Gateways I New Gateway I &lt;choose gateway type&gt;</td>
</tr>
<tr>
<td>Gateway Catalog Group</td>
<td>Gateways I &lt;click gateway name&gt; I New Group</td>
</tr>
<tr>
<td>Gateway Manager</td>
<td>Gateways</td>
</tr>
<tr>
<td>Import Installer</td>
<td>Client Configuration I Manage Installer Versions I New</td>
</tr>
<tr>
<td>Import Programs</td>
<td>Program Permissions I New Program I Import Scan</td>
</tr>
<tr>
<td>Incoming Firewall Rule</td>
<td>Policies I Manage Policy Objects I Firewall Rules I New Rule I Incoming Firewall Rule Policies I Manage Policy Objects I Firewall Rules I &lt;click rule name&gt;</td>
</tr>
<tr>
<td>Infection Events</td>
<td>Home I &lt;click a number in the Endpoint Infections table&gt;</td>
</tr>
<tr>
<td>Infection History Reports</td>
<td>Infection History</td>
</tr>
<tr>
<td>Endpoint Monitor Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Page Name</td>
<td>Location</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>Policies</td>
</tr>
<tr>
<td>Location Manager</td>
<td>Policies</td>
</tr>
<tr>
<td>Manually-Added Program</td>
<td>Program Permissions</td>
</tr>
<tr>
<td>Messaging Settings</td>
<td>Policies</td>
</tr>
<tr>
<td>Name and Notes</td>
<td>Policies</td>
</tr>
<tr>
<td>NTDomain Catalog</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Office Awareness Settings</td>
<td>Client Configuration</td>
</tr>
<tr>
<td>Outgoing Firewall Rule</td>
<td>Policies</td>
</tr>
<tr>
<td>Package Details</td>
<td>Client Configuration</td>
</tr>
<tr>
<td>Policies Using</td>
<td>Policies</td>
</tr>
<tr>
<td>Policy Assignment Report</td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td>Policy History</td>
<td>Policies</td>
</tr>
<tr>
<td>Policy Manager</td>
<td>Policies</td>
</tr>
<tr>
<td>Policy Objects</td>
<td>Policies</td>
</tr>
<tr>
<td>Policy Package</td>
<td>Policies</td>
</tr>
<tr>
<td>Ports and Protocols Manager</td>
<td>Policies</td>
</tr>
<tr>
<td>Program Group</td>
<td>Program Permissions</td>
</tr>
<tr>
<td>Program Group Permissions</td>
<td>Program Permissions</td>
</tr>
<tr>
<td>Program Groups</td>
<td>Program Permissions</td>
</tr>
<tr>
<td>Program Permissions</td>
<td>Program Permissions</td>
</tr>
<tr>
<td>Program Rules</td>
<td>Policies</td>
</tr>
<tr>
<td>Page Name</td>
<td>Location</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>RADIUS Catalog</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Role</td>
<td>Administrators</td>
</tr>
<tr>
<td>Role Manager</td>
<td>Administrators</td>
</tr>
<tr>
<td>SmartDefense</td>
<td>Policies</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Endpoints</td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>User Events Report</td>
<td>Infection History</td>
</tr>
<tr>
<td>VPN Settings</td>
<td>Client Configuration</td>
</tr>
<tr>
<td></td>
<td>Client Configuration</td>
</tr>
</tbody>
</table>
Appendix

SecureClient VPN CLI

This appendix describes an optional command-line interface (CLI) for the SecureClient VPN engine within the Endpoint Security client.

The VPN engine commands can be used to generate status information, stop and start services, or connect to defined sites using specific user profiles. Typically, endpoint users do not need to open a command prompt and use these commands, but you may wish to include the commands in a script that you transfer to remote users. This is a way to expose VPN engine operations (such as Connect/Disconnect) to external third party applications via scripting.

The general format for VPN engine commands is:

C:\> scc <command> [optional arguments]

You can use the Endpoint Security Administrator Console to include VPN functionality in an Endpoint Security client installation package. For details, see “VPN Options,” on page 158.

Table B-1: SecureClient VPN engine command line interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCC</td>
<td>VPN commands are used to generate status information, stop and start services, or connect to defined sites using specific user profiles.</td>
</tr>
<tr>
<td>scc connect</td>
<td>This command connects to the site using the specified profile, and waits for the connection to be established. In other words, the OS does not put this command into the background and executes the next command in the queue.</td>
</tr>
<tr>
<td>scc connectnowait</td>
<td>This command connects asynchronously to the site using the specified profile. This means, the OS moves onto the next command in the queue and this command is run in the background.</td>
</tr>
<tr>
<td>scc disconnect</td>
<td>This command disconnects from the site using a specific profile.</td>
</tr>
</tbody>
</table>
### Table B-1: SecureClient VPN engine command line interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scc erasecreds</td>
<td>This command unsets authorization credentials.</td>
</tr>
<tr>
<td>scc listprofiles</td>
<td>This command lists all profiles.</td>
</tr>
<tr>
<td>scc numprofiles</td>
<td>This command displays the number of profiles.</td>
</tr>
<tr>
<td>scc restartsc</td>
<td>This command restarts VPN services.</td>
</tr>
<tr>
<td>scc passcert</td>
<td>This command sets the user's authentication credentials when authentication is performed using certificates.</td>
</tr>
<tr>
<td>scc setmode</td>
<td>This command switches the VPN engine command-line mode.</td>
</tr>
<tr>
<td>scc startsc</td>
<td>This command starts VPN services.</td>
</tr>
<tr>
<td>scc status</td>
<td>This command displays the VPN connection status.</td>
</tr>
<tr>
<td>scc stopsc</td>
<td>This command stops VPN services.</td>
</tr>
<tr>
<td>scc suppressdialogs</td>
<td>This command enables or suppresses VPN engine dialog popups. By default, suppressdialogs is off.</td>
</tr>
<tr>
<td>scc userpass</td>
<td>This command sets the user's authentication credentials -- username, and password.</td>
</tr>
<tr>
<td>scc ver</td>
<td>This command displays the current VPN engine version.</td>
</tr>
<tr>
<td>scc icacertenroll</td>
<td>This command enrolls a certificate with the internal CA, and currently receives 4 parameters - site, registration key, filename and password. Currently the command only supports the creation of p12 files.</td>
</tr>
</tbody>
</table>
Index

A

accounts
  see administrators administrator authentication 186
  accounts 27–35
    creating 33
    deleting 34
    editing 34
    planning 31
    privileges 29
    roles
      creating 35
      customized 29
      default 29
      deleting 35
      editing 35
      general 29
    workflow 32
  Agent 157
  Agent clients 157
  alerts
    enabling 107
    Antisyware 121–125
    enabling 124
    enforcement 125
    introduction 121
    making exceptions 124
    overview 41
    workflow 122
  Antivirus 126–131
    configuring 130
    exceptions 122, 128
    overview 41, 127
    scan exceptions 122, 128
    scan methods 127
    scans 127
    scheduling scans 128
    targets 127
    treatment and repair 122, 128
    treatment options 122, 128
  antivirus
    see Antivirus 41
    antivirus rule, creating 109
    Apache
      starting and stopping 179
    Appscans
      creating 80
      importing 83
    arbitration
      policy 39
      assigning
        administrators 29
        authenticating
        administrators 186
        automatic client updates 136
    previewing 136
    scheduling automatic 136
    status 134
    Client Version report 171
    clients
      deleting 170
      importing 169
      new versions 157
      versions 169
    cm2.zonelabs.com 185, 186
    config.xml 156
    connected policies
      defined 37
      Cooperative Enforcement 148–154
      configuring 151
      with Restriction Firewall
        Rules 152
    cpsmi_tool.exe 156
    Creating 80
    Current Client Compliance Status report 119

C

Check Point
  VPN-1/FireWall-1 13
  Client Connectivity report 171
  client deployment options 157
  Client Diagnostic Utility 189
  client executable 156
  client installation options 163
  client logging 189
  client packages 155–169
    creating 167
    distributing 167
    download URL 169
    introduction 156
    planning your
      distribution 157
      workflow 166
  client types 157
  client update staging 134
  client updates
    acting on tested
      previews 137
      configuring test group 136
    introduction 132
    life cycle 134
    manually deploying 135
    previewing 136
    scheduling automatic 136
    status 134

D

DAT files 132
DAT update process 133
debug logging 189
Default Policy
  using 52, 53
  Default VPN Policy 162
  deploying
    policies 49
  Desktop Security Rules
    migrating to VPN 159
    disconnected policies
      defined 37
  Documentation 9
    documentation 9
    other documents 9
E
- e-mail
  - preventing attacks 146
  - protecting 41
- Endpoints
  - report 137
  - Enforcement 41
  - enforcement rules 97-118
    - adding to a policy 115
    - client 112
    - creating 108
    - deleting 113
    - editing 113
    - in policies 114
    - overview 41
    - process 98
    - tracking 119
    - enforcing client updates 169
- enterprise policies 37

F
- firewall rules 62-??
  - adding to policies 66
  - defined 63
  - deleting 68
  - editing 68
  - enabling 67
  - overview 40
  - removing from a policy 68
  - uses 62
  - workflow 65
  - Flex 157
  - Flex clients 157
  - FTP access
  - example 63

G
- gateways
  - supported 150
  - unsupported 150

H
- heartbeats 149

I
- install password 164
  - installation
  - clients 155
  - installation download site 169
  - installation packages 158
  - installing VPN 158
  - Integrations with other Check Point Products 12
  - integrity.pem 156
  - Interspect
    - intra-LAN Cooperative Enforcement 149
  - IP address
    - changing 188

J
- JDBC IP address
  - changing 188

K
- kav-integrity.zonelabs.com 134, 185, 186

L
- licensed features 177
  - licenses 177-179
  - attaching 179
  - generating 179
  - introduction 177
  - workflow 178
  - local.scv 159, 162
  - Location Awareness
    - see Office Awareness 50
  - log upload 173

M
- Mailsafe 146-147
  - manually adding programs 83
  - msi.ini file 156

N
- new features 15

O
- Office Awareness 38, 50
  - Servers 50

P
- PA
  - see Program Advisor
  - PA2.zonelabs.com 185, 186
  - packages
    - see client packages
  - packet handling, configuring 61
  - permissions 29
  - personal policies
    - defined 38
  - ping
    - blocking 69
  - policies 36-55
    - adding enforcement
      - rules 115
    - adding firewall rules 66
    - component overview 40
    - connected 37
    - creating 49
    - creating using policy
      - wizard 49
    - default 52, 53
    - deleting 55
    - deploying 49
    - disconnected 37
    - enterprise 37

198
exporting 54
managing 46–55
managing versions 54
packages 39
personal 38
policy wizard 49
removing firewall rules 68
workflow 48
policy arbitration 39
policy packages defined 39
precedence of policy rules 43
preventing e-mail attacks 146
privileges administrator 29
product.ini file 161
Program Advisor 87–96
enabling 94
overriding recommendations 95
overview 40
process 89
server 88
server process diagram 91
unknown programs 96
viewing recommendations 94
workflow 93
Program Control 69–86
adding programs 83
overview 40
progress and error messages, displaying 82
proxy configuring 184
R
RADIUS 186
reference clients 110
reports 172–174
Client Connectivity 171
Client Version 171
Current Client Compliance Status 119
Endpoints 137
restricting users with Cooperative Enforcement 149
roles see administrators
rule evaluation 43
diagram 44
S
scc connect 195
scc connectnowait 195
scc icacertenroll 196
scc listprofiles 196
scc numprofiles 196
scc passcert 196
scc startsc 196
scc status 196
scc stopsc 196
scc suppressdialogs 196
scc userpass 196
scc ver 196
scheduling client updates 136
SCV
- migrating to Endpoint Security VPN 159
SecureClient
- migrating from 158
SecureClient VPN Command Line Interface 195
silent install 164
SmartCenter
- and Administrator accounts 30
- and Administrators 32
- SmartDefense 142–145
- configuring 144
- introduction 143
- monitoring 145
- overview 41
spyware
- allowing 124
- see also Antispyware staging
- client updates 133, 134, 136
- starting Endpoint Security 179
- stopping Endpoint Security 179
T
terminating users with Cooperative Enforcement 149
third-party scripts with VPN enforcement 160
traffic how evaluated 43
U
uninstalling 180
providing 164
unknown programs managing 96
unsupported gateways 150
upd.zonelabs.com/zonealarm/online/* 134, 185, 186
updatekeyfiles.xml 156
updating clients automatic package updating 169
user.c and product.ini 156
user.c file 161
V
virus definition update process 130
viruses protecting against 126
Visitor Mode 53
VPN
- Check Point 158, 162
- Cooperative Enforcement 148
default policy for 53
importing configuration files 161
options 158
planning 161
VPN-1/FireWall-1 13
workflow 162
W
warning messages, displaying 82
workflow
system 17

Z
Zone Rules
overview 40
Zones 56-61