# Contents

## Preface
- About This Guide ................................................................. 5
- About the Endpoint Security Documentation Set .................. 5
  - Documentation for Administrators .................................... 5
  - Documentation for Endpoint Users .................................... 6
- Feedback ............................................................................. 7

## Chapter 1  **Agent and Flex**
- Architecture ......................................................................... 9
  - Endpoint Security Server .................................................. 9
  - Endpoint Security Clients .................................................. 9
- Concepts ............................................................................... 12
  - Policies ............................................................................ 12
  - Configuration Files .......................................................... 13
  - Client Packages ............................................................... 13
  - Gateways .......................................................................... 14
- Workflow ............................................................................... 15
- Windows Firewall .............................................................. 17

## Chapter 2  **GPO Distribution**
- GPO Distribution Workflow ................................................ 19
- Creating an MSI Client Package File .................................... 19
- Using the Microsoft Installer file with your GPO .................. 20

## Chapter 3  **Third-party Distribution**
- Installation Command Line .................................................. 22
  - Command-Line Components ............................................. 22
  - Command-Line Syntax ...................................................... 22
  - MSI Switches ..................................................................... 23

## Chapter 4  **Client Parameters**
- Keys and Passwords ............................................................ 25
  - Install Key ......................................................................... 25
  - User Password .................................................................... 27
- Client Parameters ............................................................... 29
- Command Line Switches ..................................................... 30

## Chapter 5  **Uninstalling Clients**
- Silently Removing a Client .................................................. 32
- Uninstalling Endpoint Security Clients ................................ 33
Uninstalling MSI files ............................................................... 33
Uninstalling using the product code ........................................... 33
Uninstalling using a script ......................................................... 33
Preface

In This Preface

About This Guide  page 5
About the Endpoint Security Documentation Set  page 5
Feedback  page 7

About This Guide

This document is the Endpoint Security Client Management Guide. Use this document to understand the Endpoint Security clients and how to install and configure them on your endpoint computers.

About the Endpoint Security Documentation Set

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

- “Documentation for Administrators,” on page 5
- “Documentation for Endpoint Users,” on page 6

Documentation for Administrators

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

| Table 1-1: Server Documentation for Administrators |
|---|---|
| **Title** | **Description** |
| Endpoint Security Installation Guide | Contains detailed instructions for installing, configuring, and maintaining Endpoint Security. This document is intended for global administrators. |
| Endpoint Security Administrator Guide | Provides background and task-oriented information about using Endpoint Security. It is available in both a Multi and Single Domain version. |
Table 1-1: Server Documentation for Administrators

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security Administrator Online Help</td>
<td>Contains descriptions of user interface elements for each Endpoint Security Administrator Console page, with cross-references to the associated tasks in the Endpoint Security Administrator Guide.</td>
</tr>
<tr>
<td>Endpoint Security System Requirements</td>
<td>Contains information on client and server requirements and supported third party devices and applications.</td>
</tr>
<tr>
<td>Endpoint Security Gateway Integration Guide</td>
<td>Contains information on integrating your gateway device with Endpoint Security.</td>
</tr>
<tr>
<td>Endpoint Security Client Management Guide</td>
<td>Contains detailed information on the use of third party distribution methods and command line parameters.</td>
</tr>
<tr>
<td>Endpoint Security Agent for Linux Installation and Configuration Guide</td>
<td>Contains information on how to install and configure Endpoint Security Agent for Linux.</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 Endpoint Security clients and how the policies they create impact the user experience.

Table 1-2: 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 client (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 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
Agent and Flex

In This Chapter

Architecture  page 9
Concepts  page 12
Workflow  page 15
Windows Firewall  page 17

Endpoint Security clients monitor your endpoints and enforce your security policies. This protects your endpoint computers and your network from security threats. This protection includes defense against both targeted and random intrusions as well as malware. Endpoint Security clients use advanced application control and sophisticated protection at the network protocol layer to neutralize threats.

It is highly recommended that you first read and understand the material in the Endpoint Security Implementation Guide before proceeding with this guide.
Architecture

The Endpoint Security system consists of two basic components:

- Endpoint Security server
- Endpoint Security clients installed on your endpoint computers

For more detailed information about Endpoint Security system architecture, including integration with other Check Point products and communications between the Endpoint Security server and the Endpoint Security clients, see the Endpoint Security Administrator Guide and the Endpoint Security Implementation Guide.

Figure 1-1: Basic Endpoint Security Architecture

Endpoint Security Server

The Endpoint Security Server allows you to centrally configure and deploy your enterprise policies through the Endpoint Security Administrator Console. You can also use the Administrator Console to pre-package Endpoint Security client executables with configuration settings and policies before you deliver them to your users.

Endpoint Security Clients

The following Endpoint Security clients are available from Check Point:

- Agent - See “Agent,” on page 10.
- Flex - See “Flex,” on page 10.
Depending on your security needs and the components you have purchased, you may be working with more than one of these client types. Although Endpoint Security clients have a lot of features in common, some administration steps and options are quite different. Be sure to use the information that pertains to the Endpoint Security client you are using.

### Agent

Use Agent when you want to centrally manage security at all times. It has a limited interface and does not allow the user to control security settings. Generally, use Agent for your less advanced users and for computers that your organization owns. Since Agent provides a simpler user interface and fewer messages to the user, it is less confusing for endpoint users.

Since Agent asks the user for less input, it can be less secure than Flex when the enterprise connected policy is not being enforced. To increase security, you may want to do one of the following:

- Set the enterprise policy to be enforced when the client is disconnected.
- Only use Agent for computers that are connected to the Local Area Network. Use Flex for computers that connect remotely and are thus exposed to more security threats.

### Flex

Use Flex when you want the endpoint user to control his or her security settings some of the time. Flex has a full user interface that allows the user to control security settings under certain conditions. Generally, use Flex for expert users who are familiar with security issues. Flex is also useful when you want to provide endpoint security for computers you do not own, but are restricted by law from exercising too much control over.

### Flex Control Center

The Flex includes a user interface called the Check Point Flex Control Center. Endpoint users use the Control Center to configure policies.

You can access the Flex Control Center by right clicking the Endpoint Security icon in the system tray and choosing **Show Client**. Use the **Help** link to access the User Guide for Endpoint Security Client Software.

### VPN Agent and VPN Flex

The Agent and Flex clients can be packaged with VPN (Virtual Private Network) functionality, in which case the client package is called VPN Agent or VPN Flex. The Endpoint Security client with VPN, also known as SecureClient, is designed to work with the Check Point VPN-1 gateway. By using it in combination with Enforcement rules, you have the option of controlling client network access at the VPN gateway. VPN
Agent and Flex also provide your endpoint users with a convenient unified interface for managing both the Endpoint Security client and their VPN access.

If you previously integrated Endpoint Security client and SecureClient by configuring SCV, be aware that the local.scv file is eliminated during endpoint installation of VPN packages. For this reason, refer to the Migrating from Check Point SecureClient section of the Endpoint Security Administrator Guide for details on recreating your prior SCV settings and Desktop Security rules with Endpoint Security.
Concepts

You will need to understand the following basic Endpoint Security system concepts in order to successfully configure and deploy your Endpoint Security clients:

- “Policies,” on page 12
- “Configuration Files,” on page 13
- “Client Packages,” on page 13
- “Gateways,” on page 14

This chapter provides an overview of these concepts. For more detailed information, see the following documents:

- Endpoint Security Implementation Guide
- Endpoint Security Administrator Guide

Policies

Policies are how you deliver security rules to your endpoint users.

Endpoint Security Administrators create enterprise policies using the Administrator Console and assign them to users or groups of users. The Endpoint Security server deploys these enterprise policies to endpoint computers, where the Endpoint Security clients receive and enforce them. You can create connected and disconnected enterprise policies for your users. If your users have Flex, they may configure a personal policy for themselves.

Policies are delivered to Endpoint Security clients as XML files.

Initial Policy

The Initial policy is the policy enforced until the first time the client contacts the Endpoint Security server. You designate this Initial policy in the client installation package so that the client has a policy before its first connection with the Endpoint Security server.

Once the client contacts the Endpoint Security server, it receives the policy package assigned to it by Endpoint Security server, which may include both connected and disconnected policies.

Connected Policies

The connected enterprise policy is the policy that is enforced when the endpoint computer is either connected to Endpoint Security server, or, if you have configured Office Awareness, connected to your network. 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 computer use policies, such as Kazaa.

Disconnected Policies

The disconnected enterprise policy is enforced when the endpoint computer is not connected to the Endpoint Security server, or to your network. Usually this policy is less restrictive, but provides a minimum level of security that you can then depend upon at all times. The goal of this 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 from the policy package assigned to a user or group of users. In the case of Flex users, their personal policy is enforced in the absence of a disconnected policy.

Personal Policies

Flex users can create their own security policies. 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.

Configuration Files

Agent and Flex also use configuration files. These files contain important information for the Endpoint Security clients, such as the location of the Endpoint Security.

Client Packages

You can use client packages to pre-configure your Endpoint Security clients and pre-populate them with security policies. Client packages not only let your endpoint users get policies and connect to Endpoint Security as soon as possible, but also lets you do things like prevent the user from uninstalling the Endpoint Security client. You can also use the packager to create a package that includes both an Endpoint Security client and VPN functionality.

Client packages contain the following files, in zipped format:

- client msi - This file installs the Endpoint Security client on your endpoint computer. The executable that is included is determined by the choice you make on the Client Package page.

- config.xml - This file provides connection information that the Endpoint Security client will use to communicate with the Endpoint Security. It also configures some aspects of how the Endpoint Security 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 on the Client Package page.
- msi.ini file - The Microsoft Installer file is used by the installer to set properties for the Endpoint Security client installation. This file is created by the client packager with the following default parameter settings:
  - REBOOT=R (no reboot)

- 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 Endpoint Security and receives its assigned policy package.

- 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 Endpoint Security client uses to receive updates.

If an Initial policy is included in the package, it is active until the Endpoint Security client connects to the Endpoint Security server. Once the Endpoint Security client connects to the Endpoint Security server, it downloads the connected and disconnected policies that are assigned to that user.

Create client packages in the Administrator Console, then use your own distribution method to deliver client packages to your endpoint computers.

For more information about creating client packages, see the Endpoint Security Administrator Guide.

**Gateways**

You can integrate Endpoint Security with supported gateways to enhance your security. Gateway integration will not be covered in this guide. The Endpoint Security Systems Requirements Document lists all the supported gateways. See the Endpoint Security Gateway Integration Guide for information about configuring your gateway to work with Endpoint Security.
Workflow

Use the following workflow with Flex or Agents. It is recommended that you familiarize yourself with the Endpoint Security Implementation Guide and set up a pilot installation before proceeding with the steps outlined here.

To use Flex or Agent:

1. Install and configure the Endpoint Security server.
   
   See the Endpoint Security Installation Guide.
   
   Do not install Endpoint Security clients and the Endpoint Security server on the same computer.

2. Create your entities.
   
   If you are using the multi-domain version of Endpoint Security, you will first need to create your domains. For more information about entities and domains, see the Endpoint Security Server Administration Guide.

3. Create your policies and assign them to your entities.
   
   For more information about creating and assigning policies, see the Endpoint Security Server Administration Guide. If your endpoint computers are using a version of Windows that includes the Windows Firewall, you should configure the policy to disable the Windows Firewall.

   Your endpoint users must be able to reach your VPN server, so be sure that all your policies, including initial and disconnected policies, permit this traffic.

   To disable Windows Firewall:
   
   a. Go to Policies.
   
   b. From the Policy List, select a policy, then Click Edit.
   
   c. Click the Client Settings tab.
   
   d. In the General Connections Settings area, choose Disable the Windows Firewall.
   
   e. Save and deploy the policy.

4. Distribute your Endpoint Security clients to your endpoint computers.

   You can use any of the following distribution methods:
   
   • Via client package - You can use the Client Packager in the Endpoint Security Administrator Console to distribute a client executable that includes one or more policy files. You can then send the URL of this policy package to users, so they can download and install the preconfigured Endpoint Security client. For more information about creating and distributing client packages, see the Endpoint Security Administrator Guide.
- Via your GPO. See “GPO Distribution,” on page 18
- Using another third-party distribution method. See “Third-party Distribution,” on page 21

If you are upgrading Agent or Flex, you can use the automatic upgrade feature in conjunction with an Enforcement rule to automatically upgrade the client when your endpoint user attempts to connect to your network. See the Endpoint Security Administrator Guide.

Distributing Endpoint Security clients by making an image of a reference computer is not supported.

If the endpoint computer is not being administered as a member of a domain, the Windows XP Security Center will show an indication that the Endpoint Security client is installed and running.
If the computer is a member of a domain, the Windows security center will not indicate that Endpoint Security client is installed and active. This is because in a domain security is assumed to be centrally managed.
Windows Firewall

Microsoft Windows XP with SP2 includes an integrated personal firewall. However, Check Point recommends that only one firewall be run on an endpoint. Microsoft has made a similar recommendation. You can configure the Endpoint Security client to shut down the Windows firewall using the Microsoft-provided API, and restart the Windows firewall if Endpoint Security client is shut down.

Whether SP2 is installed on a computer already running Endpoint Security client version 5.0.556.144 or later, or the Endpoint Security client is installed on an endpoint that already has SP2 installed, the behavior is similar:

- Endpoint Security will shut down the Windows firewall after the post-SP2 installation restart.
- If the Endpoint Security client is shut down after SP2 is installed, the client notifies Windows that it is being shut down, and Windows restarts the windows firewall.
- If Endpoint Security client is restarted, the Windows firewall is again shut down.

If a user or administrator re-enables the Windows firewall while the Endpoint Security client firewall is running, they should coexist without problems, as the two firewall operate on different system levels.

You can configure your Endpoint Security policy to disable Windows firewall using the policy. See the “Workflow,” on page 15 for more information about configuring the policy.
In This Chapter

GPO Distribution Workflow  page 19
Creating an MSI Client Package File  page 19
Using the Microsoft Installer file with your GPO  page 20

Use the instructions in this chapter to distribute an Endpoint Security client to a Group Policy Object (GPO) using a Microsoft Windows Installer package file (MSI). Be sure you are familiar with, and have tested your GPO system before performing the steps in this chapter.

Use the instructions in this chapter to install Agent or Flex on your endpoint computers. These instructions are for distributing clients to large numbers of endpoint computers at once, using a centralized distribution method. If you are installing an Endpoint Security client directly on just a few computers, see the User Guide for Endpoint Security Client Software for installation instructions.
GPO Distribution Workflow

Perform the following steps to use a Microsoft Installer Package (.msi) file to distribute Endpoint Security client using Active Directory Group Policy Objects.

In this installation, you will be creating a Microsoft Installer Package (.msi) file. You need to use Windows Installer Packages, rather than standard .exe software packages because GPO cannot accept the command line switches needed for silent install with automatic reboot during software deployment.

For more information about using a GPO, see the Microsoft Website.

**The GPO distribution workflow:**

1. From the Endpoint Security administrator console, create a client installer package .exe file by configuring and exporting a client package.

   See the Endpoint Security Administrator Guide for details on configuring and exporting a client package.

   When you create new client packages to upgrade clients in your GPO distribution, create a new install key (password) each time so that clients cannot uninstall the Endpoint Security client without your permission. In a GPO distribution the install key is cached, which means that end users will not need a key to uninstall unless you have added a new install key in the upgrade package.

2. Create an MSI (Microsoft Installer) client package installer file.

   See in “Creating an MSI Client Package File,” on page 19.

3. Use the .msi client package file with your GPO.

   See “Using the Microsoft Installer file with your GPO,” on page 20.

Creating an MSI Client Package File

**To convert a client package .exe file to an MSI file:**

1. Go to the directory to which you saved the .exe file.

   For example, if the .exe file is in the downloads directory:

   ```
   cd c:\downloads
   ```

2. Run the .exe package installer with the parameter msi.

   For example:

   ```
   <client package filename>.exe msi
   ```

   where `<client package filename>` is the filename of the .exe file you exported.

   The new file, called `<client package filename>.msi`, is created.
Using the Microsoft Installer file with your GPO

Use the GPO to create a new package, using your .msi file. See ‘How to assign software to a specific group by using a Group Policy’ on the Microsoft Website. In order to apply a group policy, you must have a Domain Controller running on Windows 2000 Server (or later) with Active Directory.
Chapter

Third-party Distribution

In This Chapter

Installation Command Line page 22
MSI Switches page 23

Use the instructions in this chapter to install your Endpoint Security client using a third-party product (other than Microsoft GPO).

Use the instructions in this chapter to install or upgrade Agent and Flex your endpoint computers. The instructions in this chapter are for distributing clients to large numbers of endpoint computers at once, using a centralized distribution method. If you are installing an Endpoint Security client directly on just a few computers, you see the Endpoint Security Administrator Guide for installation instructions.
Installation Command Line

The installer for the Endpoint Security client uses Microsoft Installer (MSI) technology. Use the command line to customize your installation or upgrade.

Command-Line Components

The installation command line consists of the following:

- **MSI switches** - These switches control the Microsoft Installer behavior. See “MSI Switches,” on page 23.
- **Endpoint Security client installation parameters** - Control the Endpoint Security client installation behaviors. See “Client Parameters,” on page 24

Command-Line Syntax

The following is the general form for the installation command lines.

```
<client package msi filename>/<MSI Switches> <Installation Parameters>
```

**Example:**

```
<client package filename>.msi INSTALLPASSWORD=psswrd
```

Note the following when creating your command lines.

- Endpoint Security client parameters must be in uppercase.
- If an Endpoint Security client parameter or MSI switch value includes a space, it must be enclosed in escape quotes.

The syntax used for the command lines in this chapter may differ from the command lines that you used in previous versions. Always use the documentation that is for the software version you are using.
MSI Switches

The installer supports all the standard MSI switches, except /j and /p. See the MSI documentation for more information about these switches. “MSI Switches,” on page 23, is provided for your convenience when working with the most common switches.

Table 3-1: MSI Switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/i &lt;file&gt;</td>
<td>Installs an msi file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Msiexec.exe /i &lt;client package filename&gt;.msi</td>
</tr>
<tr>
<td>/x &lt;GUID or file&gt;</td>
<td>Uninstalls an msi file. When uninstalling this file, you will need the product code. See “Obtaining the product code,” on page 33.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>Msiexec.exe /x &lt;client package filename&gt;.msi</td>
</tr>
<tr>
<td></td>
<td>Msiexec.exe /x {3B5F1A9D-5705-44BA-A061-C8B2DE2AF18E}</td>
</tr>
<tr>
<td>/qn</td>
<td>Silences the install. The endpoint user sees no user interface.</td>
</tr>
<tr>
<td>/qb</td>
<td>Makes the install mostly silent. Some screens appear, notifying the endpoint user of the install. This installation option requires no user input.</td>
</tr>
</tbody>
</table>

The Endpoint Security client installer automatically deactivates the Cancel button, so you do not need to suppress this button using the MSI switches.
Chapter 4

Client Parameters

In This Chapter

Keys and Passwords  page 25
Client Parameters  page 29
Command Line Switches  page 30

Use this chapter to understand the Endpoint Security client custom parameters used in GPO and other third-party distribution methods and to understand the command line switches you can use to make changes after installation.
Keys and Passwords

Since Endpoint Security clients play a critical role in providing a secure computing environment on your endpoint computers, it is essential to prevent unauthorized changes to the installation. Use passwords to prevent endpoint users from making changes. Endpoint Security clients use the following passwords:

- install key
- user password

Install Key

The install key is needed in order to uninstall or upgrade the client. A default install key (“secret”) is created if you do not set one. The install key does the following:

- Prevents endpoint user changes to the installation
  Preventing endpoint users from uninstalling the Endpoint Security client is essential to the security of your network. See “Preventing Endpoint Security Client Uninstalls,” on page 26.

- Allows administrators to perform silent upgrades and uninstalls
  Because there is always an install key (the default one or your custom one), you upgrade or uninstall the Endpoint Security client without any user interaction. On the endpoint, the Endpoint Security icon appears in the desktop system tray during the upgrade or installation, but no action is required of the user.

- Prevents endpoint users from blocking administrator-initiated upgrades and uninstalls with the user password.
  The install key overrides the user password. For more information, see “User Password,” on page 27.

Default Install Key

A default install key is created if you do not create one. The default install key is secret. An install key is required to uninstall or upgrade the client, so it prevents endpoint users from uninstalling the Endpoint Security client. For this reason, the default key is a back-up safety mechanism to protect your network from endpoint computers that are not protected by an Endpoint Security client.

If you do not set an install key when creating the client installation package, the default key is generated.

To create your own install key while creating the client package, see “Setting an Install Key,” on page 26.

If you did not create a custom install key and now have the default install key on the client, you can reset it to your own key with an upgrade. See “Changing an Install Key,” on page 27.
Preventing Endpoint Security Client Uninstalls

The install key prevents endpoint users from uninstalling the Endpoint Security client. Set the install key during the initial installation of the Endpoint Security client, and the password will be required for any subsequent changes to the installation. See “Setting an Install Key,” on page 26.

When you create new client packages to upgrade clients in your GPO distribution, create a new install key each time so that clients cannot uninstall the Endpoint Security client without your permission. In a GPO distribution the install key is cached, which means that end users will not be asked for the key if they try to uninstall, unless you have added a new install key in the upgrade package.

It is highly recommended that you set a custom, unique install key whenever you install an Endpoint Security client. This prevents endpoint users from uninstalling the Endpoint Security client and allows you to perform silent upgrades and uninstalls.

Allowing endpoint computers that are not protected by an Endpoint Security client to connect to your network is a security risk.

If you do not set a custom, 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 Endpoint Security client is not running. This prevents the endpoint user from removing the Endpoint Security client and then connecting to your network while unprotected. See the Endpoint Security Administrator guide for more information about cooperative enforcement with supported gateways.

Setting an Install Key

If you do not set the install key for the initial Endpoint Security client install, it is set the default install key, secret.

To set the install key:

1. Use the appropriate method to configure the install key:
   
   • If you are using GPO, configure the install key (password) using the Endpoint Security administrator console when you create the client installation package.
   
   • If you are using another third-party distribution method, you can also set the install key using an installation command line. See “Installation Command Line,” on page 22.
      
      Example:

      ```
      msiexec /i <client package filename>.msi NEWINSTALLPASSWORD=<yourpassword>
      ```

2. Record the password.
   
   If you lose this password you will be unable to change it or perform silent upgrades or uninstalls.
Changing an Install Key

You can modify a password when doing an upgrade of an existing installation. To do this you must supply both the new install key (password) and the old one.

The default install key, which you need to use if you did not establish one during the initial installation, is secret.

To change the install key:

1. Do one of the following:
   - If you are using GPO, configure the install key in the Endpoint Security administrator console when you create the client installation package.
   - If you are using another third-party distribution method, you can also configure the install key using an installation command line. See “Installation Command Line,” on page 22.
     
     Example:

     ```
     Msiexec /I <client package filename>.msi INSTALLPASSWORD=<newpassword>
     NEWINSTALLPASSWORD=<oldpassword>
     ```

2. Record the new install key.

   If you lose this install key you will be unable to change it or perform silent upgrades or uninstalls.

If you are using a client package to install the Endpoint Security client, you can also set the install key using the Install Key option in the Client Packager

User Password

Flex provides the endpoint user with the option of setting a password. This enables the endpoint user to stop anyone who does not know the password from changing their personal policies.

You, as the administrator, can also set the user password during installation for many endpoint computers at once, or your can set it individually on each endpoint computer using the Check Point Flex Control Center. You may want to do this to prevent personal policy changes. Generally, administrators do not need to set this password, but it is important to understand that the install key takes precedence over the user password.

About the Relationship Between the Install Key and User Password

The install key prevents unauthorized uninstalls or upgrades. If the user password is set and an upgrade or uninstall is run with the install key only, then the user password will not block the change. The install key overrides the user password. To prevent your endpoint users from blocking your upgrades or uninstalls, it is highly recommended that you create a custom, unique install key.
Preventing Personal Policy Changes

The recommended way to prevent endpoint users from making changes to policies is to deploy Agent to those users. However, if you want to use Flex but still prevent users from changing their personal policies, you can set a user password during installation and supply the password only to certain endpoint users.

This allows endpoint users to see the endpoint user interface available in Flex, but not make changes. It also allows you to make changes directly on the endpoint computer using the Check Point Flex Control Center, should you decide to do so.

To set a user password:

1. Do one of the following:
   - If you are using GPO, configure the user password for the Endpoint Security client installer using the Endpoint Security administrator console when you create the package.
   - If you are using another third-party distribution method, you can also configure the parameter using an installation command line. See “Installation Command Line,” on page 22.
     
     Example:

     msiexec /i <client package name>.msi NEWUSERPASSWORD=<yourpassword>

2. Record the password.

   If you do not record this password you will be unable to change it.

To change the user password:

1. Use the appropriate method to change the user password:
   - If you are using GPO, change the user password for the Endpoint Security client installer using the Endpoint Security administrator console when you create the package.
   - If you are using another third-party distribution method, you can configure the parameters using an installation command line. See “Installation Command Line,” on page 22.
     
     Example:

     msiexec /i <client package name>.msi USERPASSWORD=<newpassword>
     NEWUSERPASSWORD=<oldpassword>

2. Record the new password.

   If you lose this password you will be unable to change it.
# Client Parameters

Use the following client parameters to customize installation. The default value given is the default given in the msi file. If you are using Client parameters in a command line, note that they must be in uppercase, preceded by the /v switch and enclosed in quotation marks.

**Table 4-1: Client Parameters**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENTSTARTUP</td>
<td>Triggers the Endpoint Security client to start up after installation.</td>
<td>Yes</td>
</tr>
<tr>
<td>FORCEREBOOTDIALOG</td>
<td>Warns the user that an installation reboot will occur in ( n ) number of minutes, where is ( n ) is specified by REBOOTDELAY. The user cannot cancel this reboot, and user input is not required.</td>
<td>No</td>
</tr>
<tr>
<td>INSTALL_SD</td>
<td>Installs the SmartDefense feature. If INSTALL_VPN=YES, INSTALL_SD must be YES.</td>
<td>Yes</td>
</tr>
<tr>
<td>REBOOTDELAY</td>
<td>Number of minutes between FORCEREBOOTDIALOG warning and reboot. The maximum value for this command is 15.</td>
<td>1</td>
</tr>
<tr>
<td>REGISTRYFILE</td>
<td>Location of the .reg file describing registry entries to make during the installation.</td>
<td>Blank</td>
</tr>
<tr>
<td>RESETVPNCONFIG</td>
<td>Removes the existing user VPN settings. Other Endpoint Security client settings are maintained.</td>
<td>No</td>
</tr>
</tbody>
</table>
Command Line Switches

Use command line switches to make changes to your Endpoint Security clients after installation.

To use command line switches:

1. Open a command line window.
   - By default this is C:\Program Files\CheckPoint\Integrity Client.
3. Type `iclient -<switch> <parameter>`
   - Example: `iclient -config path_to_config.xml -pwinst installpassword`
   - If the parameters contain spaces, you must enclose them in double quotes. For information about the most commonly used switches and parameters, see Table 4-2: Command Line Switches.
4. Close the command line window.

Table 4-2: Command Line Switches

<table>
<thead>
<tr>
<th>Switches and Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-serialnumber or -lickey</td>
<td>Inserts the key into the license table.</td>
</tr>
<tr>
<td>-password</td>
<td>Specifies the user password.</td>
</tr>
<tr>
<td>-pwinst</td>
<td>Use this parameter to specify the old install key when changing it using the -setpwinst or -pwinstset parameters.</td>
</tr>
<tr>
<td>-upgradekey</td>
<td>Specifies the upgrade key.</td>
</tr>
<tr>
<td>-setpass or -passwset</td>
<td>Sets a new user password. Use the -password parameter to specify the old password.</td>
</tr>
<tr>
<td>-setpwinst or -pwinstset</td>
<td>Changes the install key. These parameters can only change existing install keys. If you did not specify an installation password when you first installed the Endpoint Security client, you will not be able to use these parameters to set it.</td>
</tr>
<tr>
<td>-config &lt;path to config file&gt;</td>
<td>Applies the configuration file to the personal policy. Use this to specify Endpoint Security connection information.</td>
</tr>
<tr>
<td>-policy &lt;path to policy file&gt;</td>
<td>Applies the policy file to the enterprise connected policy.</td>
</tr>
<tr>
<td>-disconnectedPolicy &lt;path to policy file&gt;</td>
<td>Applies the policy file to the enterprise disconnected policy.</td>
</tr>
<tr>
<td>-HU100</td>
<td>Regenerates the HU100 key that uniquely identifies the endpoint. Use this if you have erroneously used imaging to install Endpoint Security clients.</td>
</tr>
<tr>
<td>-errorssubmission</td>
<td>Zips all errors, logs, and dumps and sends them to Check Point for analysis.</td>
</tr>
</tbody>
</table>
Chapter 5

Uninstalling Clients

In This Chapter

Silently Removing a Client  page 32
Uninstalling Endpoint Security Clients  page 33

Use these instructions to uninstall Endpoint Security clients on a large number of endpoint computers. For information about uninstalling an Endpoint Security client on just one computer, see the User Guide for Endpoint Security client Software. You must have administrator privileges to uninstall Endpoint Security clients.
Silently Removing a Client

You can silently uninstall Endpoint Security clients to reduce the need for endpoint user cooperation. By default, running a silent uninstallation automatically restarts the endpoint computer without warning to complete the installation process. However, you can use additional parameters and switches to either suppress the restart, or to prompt the endpoint users to restart the endpoint computers themselves. For more information about these parameters and switches, see:

- “MSI Switches,” on page 23.
- “Client Parameters,” on page 24
Uninstalling Endpoint Security Clients

Use one of the command lines described in the following sections to uninstall Endpoint Security clients. The method that you use to uninstall the Endpoint Security clients depends on the method you used to install them.

You cannot uninstall Endpoint Security clients using GPO. Uninstall GPO-installed Endpoint Security clients using the product code, using either the command line or a script. See “Uninstalling using the product code,” on page 33 and “Uninstalling using a script,” on page 33.

Uninstalling MSI files

Use the following command line to uninstall the Endpoint Security client if you know which specific MSI file you used to install it:

Msiexec /X /qn <installDatabase.msi> INSTALLPASSWORD=<password>

Uninstalling using the product code

Use the following command line to uninstall the Endpoint Security client if you do not know the specific file you used to install it:

Msiexec /X /qn <Product Code> INSTALLPASSWORD=<password>

Obtaining the product code

To obtain the product code, (GUID), examine this registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm\MsiProductCode.

The product key is the value for MsiProductCode. You can verify this code by checking for a subfolder named with the product key.

Uninstalling using a script

You can also uninstall the Endpoint Security client using a script. The following sample script automatically finds the product code and uses it to uninstall the MSI file. The script then causes the computer to reboot.

Dim runPath, strReadValue
Dim objShell

Set objShell = CreateObject("WScript.Shell")

Const Reg_TestKey = "HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm\MsiProductCode"

strReadValue = objShell.RegRead(Reg_TestKey)
runPath = "msiexec /x " & strReadValue & " /qn INSTALLPASSWORD=secret"

Set WshShell = CreateObject("WScript.Shell")

WshShell.Run runPath

wscript.quit
uninstallation
  MSI switch 23
uninstalling 31
  command lines 33
  preventing 26
  silently 32
upgrading
  Agent 16
  automatic 16
  Flex 16
user interface
  Control Center 10
user password 27

Windows Firewall 17
Windows XP 17
Windows XP Security Center 16
workflow
  Agent 15
  Flex 15