Integrity Advanced Server

Gateway Integration Guide

Version NGX 6.6

1-0273-0660-2006-02-24

Contents

Preface

This preface provides an overview of Integrity Advanced Server documentation.

It contains the following topics:

About this Guide

This guide describes the steps necessary to integrate your gateway device with Integrity Advanced Server. Integrating your gateway with Integrity Advanced Server enables you to use the Cooperative Enforcement™ feature for remote access protection. Please make sure you have the most up-to-date version available for the version of Integrity Advanced Server that you are using.

Before using this document, you should read and understand the information in the *Integrity Advanced Server Administrator Guide* in order to familiarize yourself with the Cooperative Enforcement feature.

Other Documentation

You should familiarize yourself with the other documentation that is available for Integrity Advanced Server, including the documentation for the Integrity clients. This documentation includes:

Server Documentation for Administrators

The following documentation is intended for use by Integrity Advanced Server administrators when using the server.

Table 4-1: Server Documentation for Administrators

Title	Description
Integrity Advanced Server Installation Guide	Contains detailed instructions for installing, configuring, and maintaining Integrity Advanced Server. This document is intended for global administrators.
Integrity Advanced Server Administrator Guide	Provides background and task-oriented information about using Integrity Advanced Server. It is available in both a Multi and Single Domain version.
Integrity Advanced Server Administrator Online Help	Contains descriptions of user interface elements for each Integrity Advanced Server Administrator Console page, with cross-references to the associated tasks in the Integrity Advanced Server Administrator Guide.
Integrity Advanced Server Implementation Guide	Contains an overview of Integrity Advanced Server features and concepts. It also explains how to plan your security policies, and provide support to endpoint users.
Integrity Advanced Server System Requirements	Contains information on client and server requirements and supported third party devices and applications.

Client Documentation for Administrators

The following documentation is intended for use by Integrity Advanced Server administrators and describes how to change the XML policy file and installer behavior without the use of the Administrator Console.

Table 4-2: Client Documentation for Administrators

Title	Description
Integrity XML Policy Reference Guide	Contains detailed information on the contents of Integrity client XML policy files. You can use this guide to make direct changes to XML policies, without using the Integrity Advanced Server Administrator Console.
Integrity Client Management Guide	Contains detailed information on the use of command line parameters to control Integrity client installer behavior and post-installation behavior.
Integrity Client Support Utility Guide	The Client Log Upload Utility provides a way for a user to assist technical support personnel by uploading Integrity client diagnostic information to a pre-defined location.

Client Documentation for Endpoint Users

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

Table 4-3: Client documentation for endpoint users

Title	Description
User Guide for Integrity Client Software	Provides task-oriented information about the Integrity clients (Agent, Flex, and Desktop) as well as information about the user interface.
Introduction to Integrity Flex	Provides basic information to familiarize new users with Integrity Flex. This document is intended to be customized by an Administrator before distribution. See the Integrity Advanced Server Implementation Guide for more information.
Introduction to Integrity Agent	Provides basic information to familiarize new users with Integrity Agent. This document is intended to be customized by an Administrator before distribution. See the Integrity Advanced Server Implementation Guide for more information.

Chapter 1

Gateway Integration Overview

This book describes the steps necessary to integrate your gateway device with Integrity Advanced Server. Integrating your gateway with Integrity Advanced Server enables you to use the Cooperative Enforcement™ feature for remote access protection.

Prerequisites

This book only describes the integration steps specific to each gateway device. You must also perform the steps for configuring the Cooperative Enforcement feature as described in the *Integrity Advanced Server Administrator Guide*. You will also need to have a general understanding of networking concepts. It is recommended that you have your gateway already configured to work with your network before beginning and that you have tested your setup.

System Requirements

For all System Requirements and version information for supported gateways, see the Integrity Advanced Server System Requirements document.

Chapter 2

Network Access Server Integration

This chapter describes how to set up Integrity Advanced Server's Cooperative Enforcement feature for an 802.1x-compatible network access server (NAS). To enable Cooperative Enforcement, you must configure the:

- RADIUS server
- Integrity Advanced Server
- 802.1x-compatible NAS
- endpoint computer

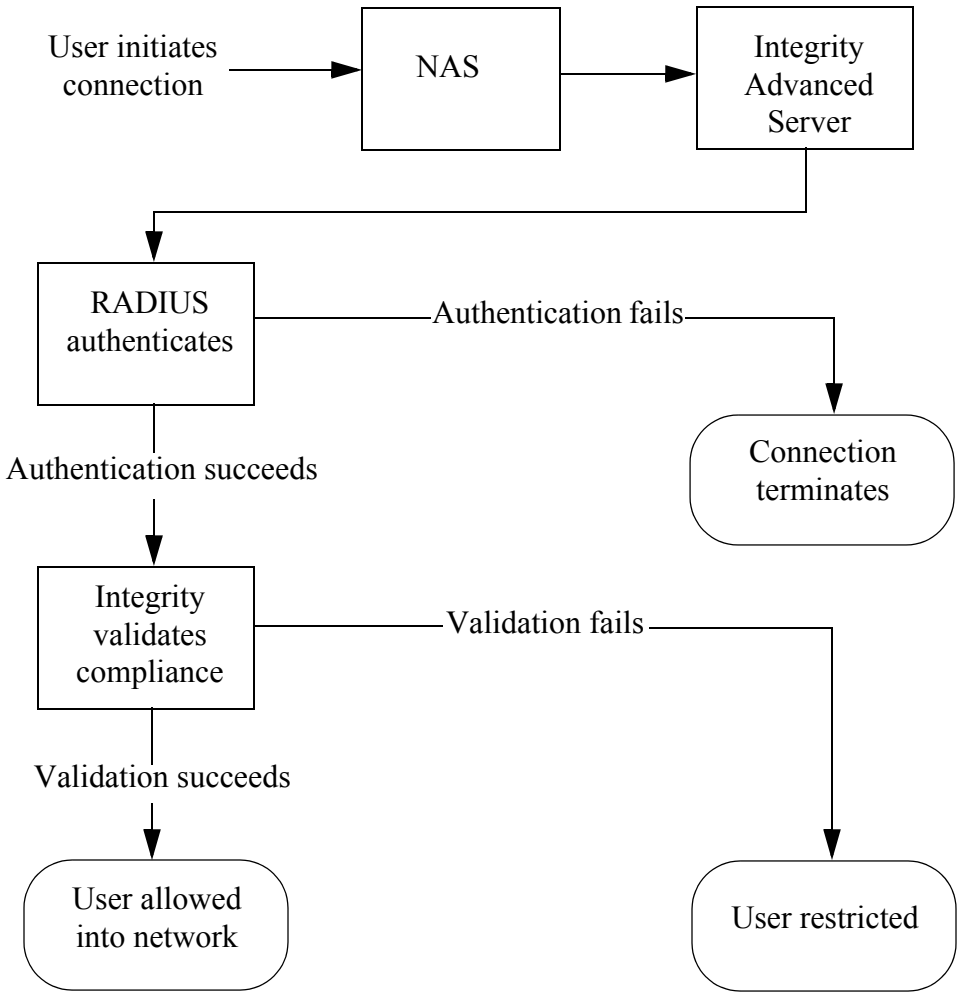
This chapter covers configuration of the RADIUS server, Integrity Advanced Server, and the endpoint computer. For information about configuring your NAS, see the appropriate vendor-specific chapter. (Vendor-specific chapters are listed in "Configuring the NAS," on page 24.)

The following topics are covered:

The instructions in this chapter assume you have already installed and performed the initial configuration on a supported NAS and a supported RADIUS server.

Understanding Cooperative Enforcement Architecture

The Cooperative Enforcement system architecture allows for a variety of different configurations. This section describes how the components interact to provide cooperative enforcement.



1. A user opens a connection to the NAS.
2. The NAS directs the connection to Integrity Advanced Server.
3. Integrity Advanced Server forwards the authentication request to the RADIUS server.
4. If authentication
   a. **succeeds**, Integrity Advanced Server can communicate with the endpoint computer.
   b. **fails**, the connection terminates.

5 Integrity Advanced Server checks the endpoint computer's compliance. If the client is

   a **compliant**, the client is granted access to the corporate network.

   b **not compliant**, the client is restricted to an isolated Virtual Local Area Network (VLAN) or to the Sandbox, or traffic is limited to specific destination IP addresses, ports, and protocols. You can also configure Integrity to reject connections for non-compliant endpoints that attempt to connect to the network through a wireless access point (as opposed to a switch). (For information about rejecting the connection, see the sections on gateway catalogs in the *Integrity Advanced Server Administrator Guide* and the associated online help. For more information about the Sandbox, see the ***Installation and Configuration Guide***.)

Configuration Overview

This section discusses the information you will need before starting the configuration, and it lists the necessary configuration procedures.

Before You Begin

Before you begin, gather the following information for each NAS-type / RADIUS combination in your system:

- Port and IP Address for:
  - Integrity Advanced Server
  - RADIUS server or distributed RADIUS proxy server
- RADIUS shared secret
- NAS shared secret
- NAS IP address
- VLAN ID and Filter name (depending on NAS support)
- Any vendor-specific attributes (VSAs) for your NAS

Configuring Cooperative Enforcement

This section lists the procedures you must perform to enable Cooperative Enforcement. The individual procedures are covered in the sections that follow.

To configure Cooperative Enforcement with an 802.1x-compatible NAS:

1 Configure the RADIUS server. ***See page 18.***

   a Configure the NAS as a RADIUS client. ***See page 18.***

   b Configure Integrity as a RADIUS client. ***See page 19.***

   c Configure Integrity access to the RADIUS server. ***See page 20.***

2 Configure Integrity Advanced Server. ***See page 23.***

   a Enable 802.1x communication. ***See page 23.***

   b Create a catalog for the gateway. ***See page 23.***

   c Assign a policy to the gateway catalog. ***See page 23.***

3 Configure the NAS. ***See page 24.***

4 Configure the endpoint computer. ***See page 25.***

Configuring the RADIUS Server

This section explains how to configure the RADIUS server. Perform these steps for each NAS that proxies authentication to the RADIUS server.

The examples in this section use Microsoft's Internet Authentication Service. If you are using a RADIUS server other than the Internet Authentication Service, consult your product documentation for instructions on adding a RADIUS client.

To configure the Internet Authentication Service:

1. Configure the NAS as a RADIUS client. ***See page 18.***
2. Configure Integrity as a RADIUS client. ***See page 19.***
3. Configure Integrity access to the RADIUS server. ***See page 20.***

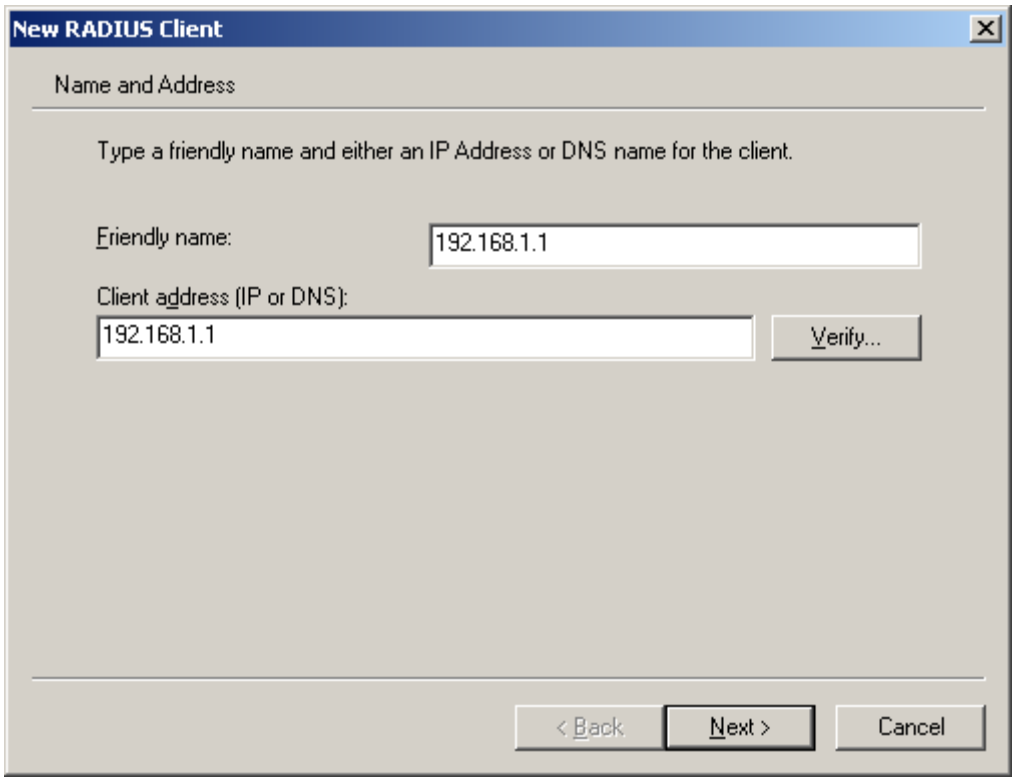
Configuring the NAS as a RADIUS Client

On the RADIUS server, configure the NAS as a RADIUS client.

To add the NAS as a RADIUS client:

1 Open Internet Authentication Service, expand **RADIUS clients**, and choose **New RADIUS Client**.

The New RADIUS Client window opens. Enter the new RADIUS client information as follows:



a In the **Friendly name** field, enter the friendly name for the NAS.

b In the **Client address (IP or DNS)** field, enter the IP address of the NAS.

2 Click **Next**.

The Additional Information window opens.

3 Enter the RADIUS shared secret, re-enter the secret in the confirmation box, and click **Finish**.

The NAS appears in the RADIUS client list.

4 Verify the configuration by right-clicking the NAS RADIUS client entry and choosing **Properties**.

Configuring Integrity as a RADIUS Client

Integrity Advanced Server handles authentication requests to the RADIUS server.

To add Integrity as a RADIUS client:

1 Open Internet Authentication Service, expand **RADIUS clients**, and choose **New RADIUS Client**.

The New RADIUS Client window opens.

2 Enter the client information as follows:

a In the **Friendly name** field, enter **Integrity Advanced Server**.

b In the **Client address (IP or DNS)** field, enter the IP address of Integrity Advanced Server.

3 Click **Next**.

The Additional Information window opens.

4 Enter the RADIUS shared secret, re-enter the secret in the confirmation box, and click **Finish**.

Integrity Advanced Server appears in the RADIUS client list.

Make note of the RADIUS secret you enter for the client, as you must enter the same secret when configuring the gateway on Integrity Advanced Server.

5 Verify the configuration by right-clicking the Integrity Advanced Server RADIUS client entry and choosing **Properties**.

Configuring Integrity Access to the RADIUS Server

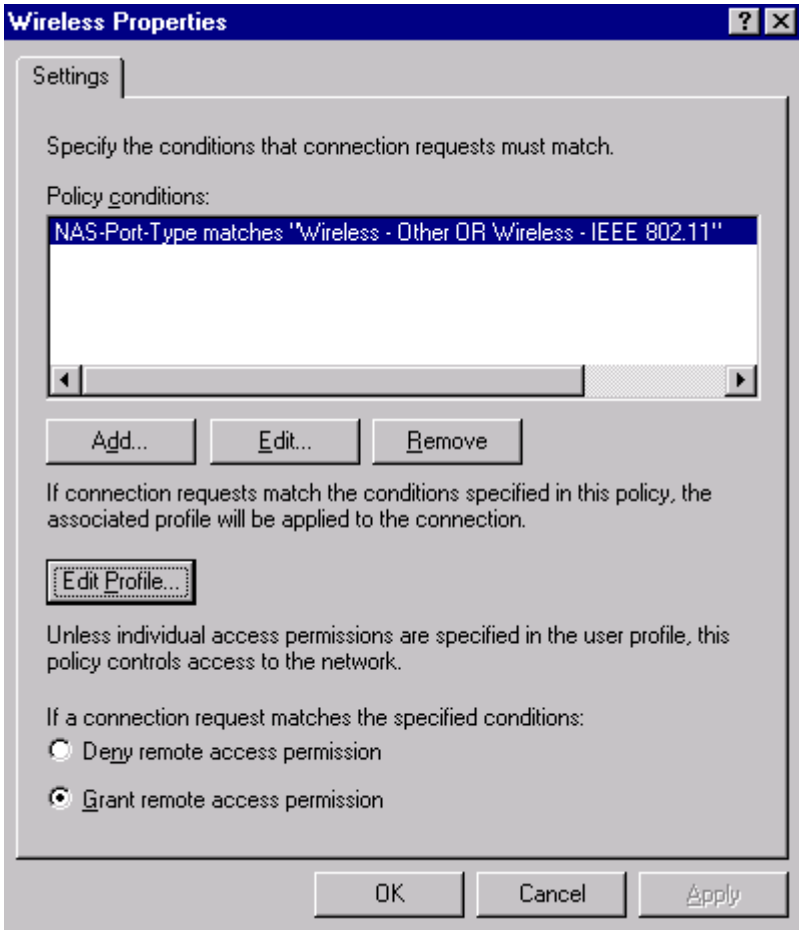
To configure Integrity access to the RADIUS server:

1 In the Internet Authentication Service left panel, select **Remote Access Policies**.

The Remote Access Policies appear in the right panel.

2 Right-click **Connections to Microsoft Routing and Remote Access server** and choose **Properties**.

The Wireless Properties window appears.



3 In the Policy Conditions area, set the conditions that are appropriate for your organization. (The example above shows the default setting.)

4 Select **Grant remote access permission** and click **Edit Profile**.

The Edit Dial-in Profile window opens.

5 Select the following settings from the Authentication tab:

- **Microsoft Encrypted Authentication version 2 (802.1x)**
  - **User can change password after it has expired**
- **Microsoft Encrypted Authentication (MS-CHAP)**
  - **User can change password after it has expired**

6 Click **EAP Methods**.

A list of the EAP types that are configured with the policy appears.

7 Remove all EAP types except the one you plan to use. (You can only specify one EAP type per NAS.)

8 Click **OK** to save your changes. Click **OK** in each window to close all except the main Internet Authentication Service window.

9 Restart the Internet Authentication Service to register the new configuration. To do so, right-click **Internet Authentication Service** (in the left panel) and choose **stop**, and then right-click it again and choose **start**.

10 Right-click **Internet Authentication Service** (local) and select **Register Server in Active Directory**. IAS can now authenticate users from your AD domain.

Configuring Integrity Advanced Server

This section describes how to configure Integrity Advanced Server to work with an 802.1x-compatible NAS.

To configure the Integrity Server:

1 Enable 802.1x communication. ***See page 23.***

2 Create a catalog for the gateway. ***See page 23.***

3 Assign a policy to the gateway catalog. ***See page 23.***

Enabling 802.1x Communication

To enable 802.1x communication:

1 In the Integrity Advanced Server administration console, go to **System Configuration** | **Server Settings** | **Edit**. (If your Integrity installation has multiple domains, do this in the System Domain.)

2 Under 802.1x Settings, select **Configure Settings for Enabling 802.1x**.

3 Type the RADIUS authentication port number and the RADIUS secret.

4 Click **Save**.

Creating a Catalog for the Gateway

Create a gateway catalog for your NAS. This lets you apply a specific policy to all users who access the network through that NAS. For information about creating a gateway catalog, see the *Integrity Advanced Server Administrator Guide* and the associated online help.

Assigning a Policy to the Gateway Catalog

Assign a policy to your new gateway catalog. Users who log in through the relevant NAS will receive the assigned policy. For information about creating and assigning policies, see the *Integrity Advanced Server Administrator Guide*.

Configuring the NAS

After configuring the RADIUS server and Integrity Advanced Server according to the instructions in this chapter, you must configure the NAS and the endpoint computers. To configure the NAS, see the appropriate vendor-specific chapter:

- "Configuring the Cisco Aironet 1100 Series Wireless Access Point," on page 100
- "Configuring the Cisco Catalyst 2950," on page 107
- "Configuring the Enterasys RoamAbout R2," on page 113
- "Configuring the Check Point Safe@Office 425W," on page 119

After you configure the NAS, return to this chapter and configure the endpoint computers as described in the next section.

Be sure to set the reauthentication intervals on all switches and wireless access points to five minutes or more.

Configuring Endpoint Computers

Endpoint configuration varies, depending on whether the endpoint will connect to the network through a wireless access point or through a wired connection. Perform the configuration that is appropriate for your setup:

- "Configuring Endpoints for Use with Wireless Access Points," on page 25
- "Configuring Endpoints for Use with Wired Connections," on page 30

These instructions assume that the user-based certificate and either Integrity Flex or Integrity Agent version 6.0 are installed on the endpoint computer. For information on deploying the Integrity client to endpoint computers see the ***Integrity Client Management Guide***. Be sure to reboot the endpoint computer after installing the Integrity client. If you do not restart the computer, you will not be able to configure the connection.

Configuring Endpoints for Use with Wireless Access Points

This section explains how to configure endpoint computers for Cooperative Enforcement when you are using a wireless access point.

To configure the connection:

1. "Select the Service Set Identifier (SSID)," on page 25
2. "Set the Association Properties," on page 26
3. "Set the Authentication Properties," on page 28

Select the Service Set Identifier (SSID)

To set the SSID:

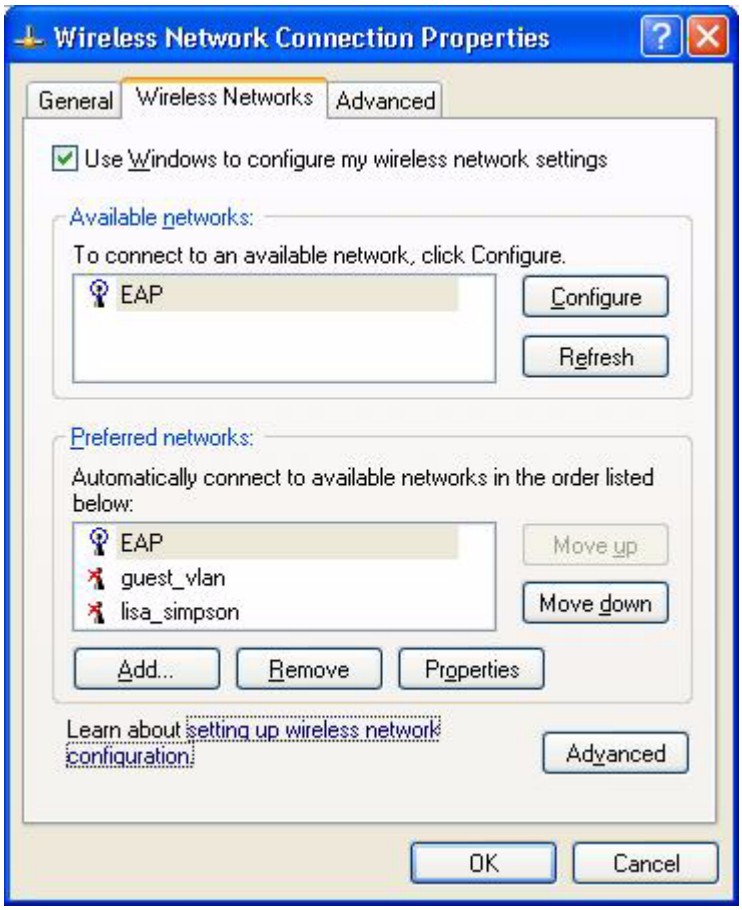
1. Insert the wireless networking card.

   The connection automatically opens.
2. Open the Network Connection manager.
3. Right-click the wireless network connection and choose **Properties**.

   The Wireless Network Connection Properties window appears.

4 Click the **Wireless Networks** tab.

A list of the available connection SSIDs appears.



If the desired SSID is not listed, click **Advanced**, enter the SSID, and click **OK**. The SSID now appears in the list.

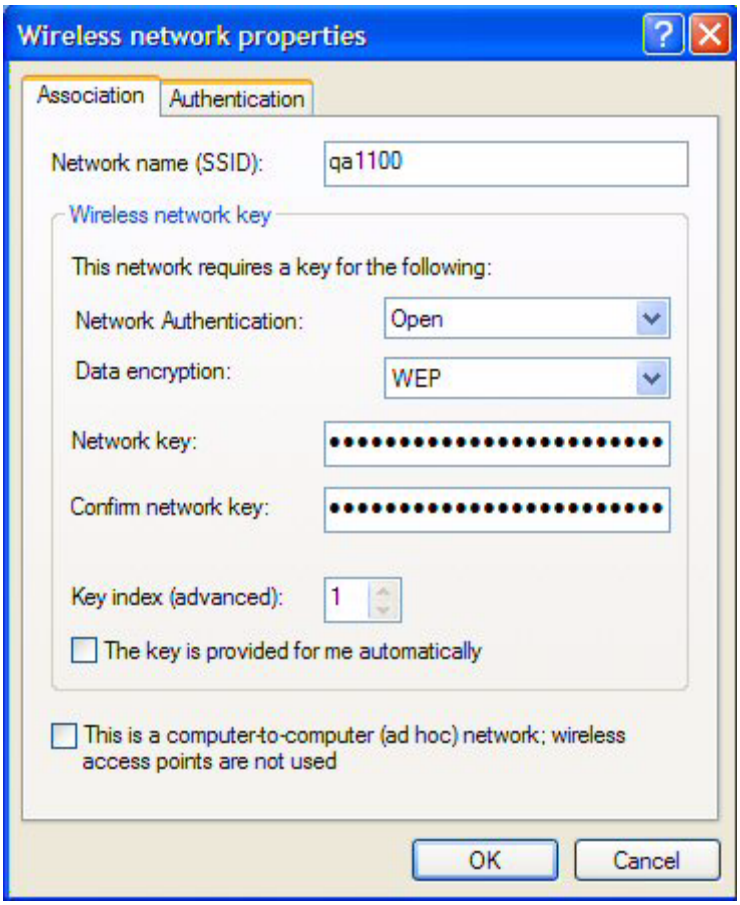
5 Select the SSID you created on the gateway and click **Configure**.

The Wireless Network Properties window appears.

Set the Association Properties

To set the association properties:

1 Go to the **Association** tab.



2 In the Network Authentication dropdown list, select **Open**.

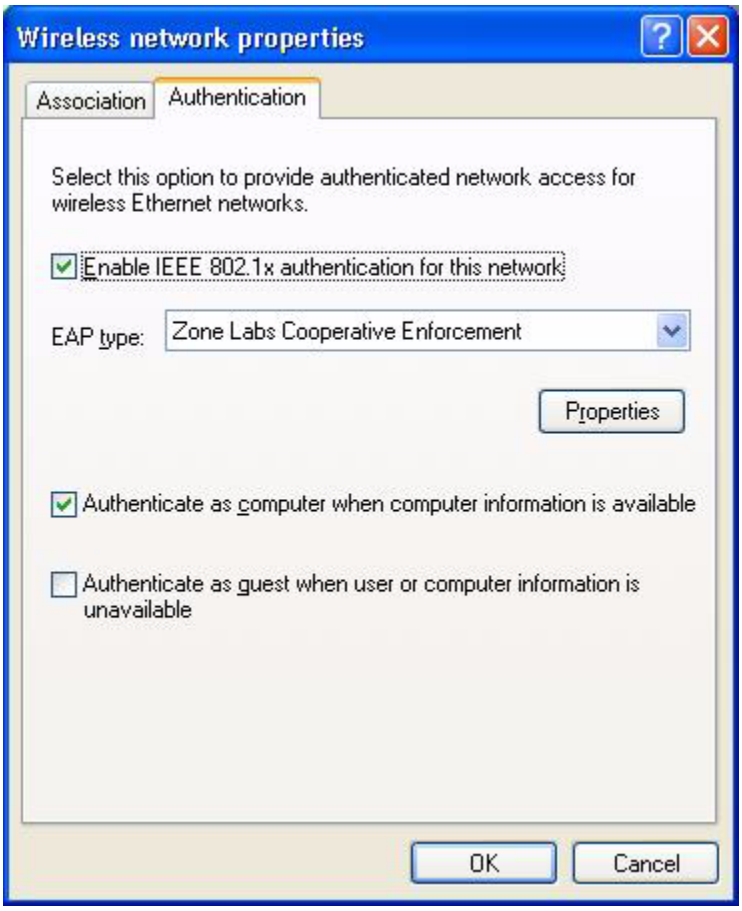
3 In the Data Encryption dropdown list, select **WEP**.

4 In the Network Key field, enter the WEP network key you created on the gateway. Type the WEP network key a second time in the Confirm Network Key field.

Set the Authentication Properties

To set the authentication properties:

1 Go to the **Authentication** tab.



2 Select the **Enable IEEE 802.1x authentication for this network** checkbox.

3 In the EAP type dropdown list, select **Zone Labs Cooperative Enforcement** and then click **Properties**.

The Zone Labs Cooperative Enforcement appears in the EAP type drop-down list only if Integrity client version 6.0 is installed on the endpoint computer.

The Zone Labs Cooperative Enforcement properties window appears.

4 In the Choose an EAP Type to Use for Authenticating the User dropdown list, do one of the following:

- Select **Smart Card or other Certificate** and click **Properties**. Go to step 5.
- Select **Protected EAP (PEAP)** and click **Properties**. Go to step 6.

Do *not* choose **Secured Password** from the dropdown list, as that option is not supported. If you wish to use a secured password, choose **Protected EAP (PEAP)** and then, in step 6, select **Secured password** as the authentication method.

5 If you chose Smart Card or other Certificate, the Smart Card or Other Certificate Properties window appears.

In the When Connecting area of the properties window, make sure to *uncheck* the **Validate server certificate** checkbox. Then select **Use a certificate on this computer**. Go to step 8.

6 If you chose Protected EAP (PEAP), the Protected EAP Properties window appears. Do the following:

- In the When Connecting area, make sure to *uncheck* the **Validate server certificate** checkbox.
- In the Select Authentication Method dropdown list, choose the appropriate authentication method (**Secured password** or **Smart Card or other Certificate**) and click **Configure**.

The appropriate configuration dialog box appears.

7 Do one of the following:

- If you chose Secured password (EAP-MSCHAP v2), select the appropriate setting for **Automatically use my Windows login name and password...** (Generally, this checkbox should remain selected. If you do not plan to log in to the domain,

however, uncheck this checkbox. This causes Integrity to prompt you for your domain credentials when you log in to the endpoint.)

- If you chose Smart Card or other Certificate, make sure to *uncheck* the **Validate server certificate** checkbox (in the When Connecting area), and then select **Use a certificate on this computer**.

8 Click **OK** in all relevant windows to save your changes and close the Network Connection manager.

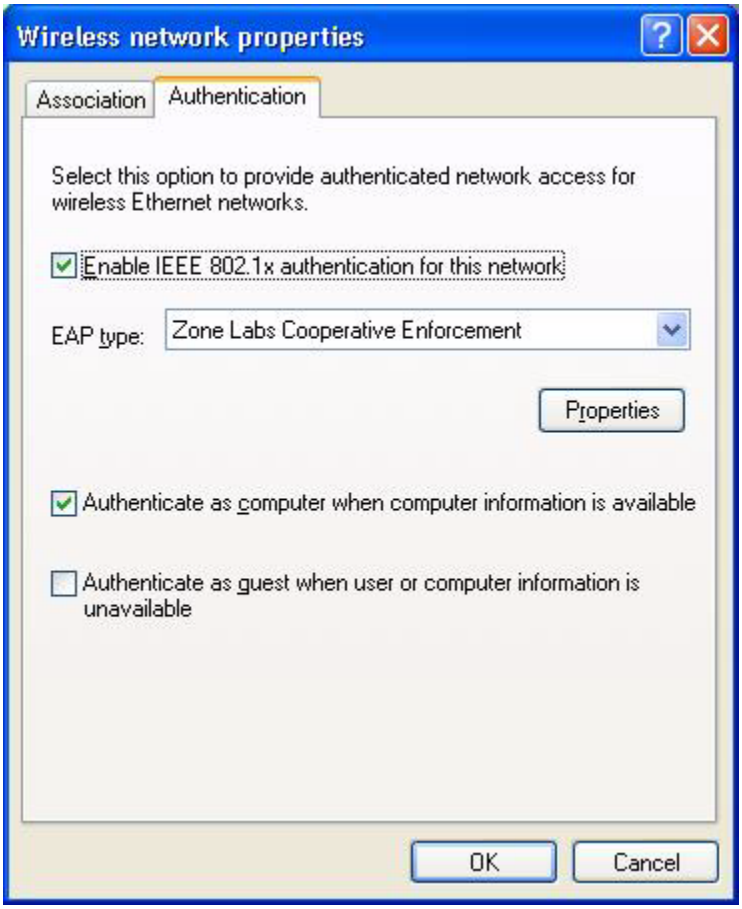
The endpoint computer can now connect using Cooperative Enforcement.

Configuring Endpoints for Use with Wired Connections

If the endpoint computer connects to the network through a wired connection, perform the configuration steps in this section.

To configure the connection:

1 In the Network Connections manager, right-click on the desired local area connection, select **Properties**, and click the **Authentication** tab.



2 Select the **Enable IEEE 802.1x authentication for this network** checkbox.

3 In the EAP type dropdown list, select **Zone Labs Cooperative Enforcement** and then click **Properties**.

The Zone Labs Cooperative Enforcement appears in the EAP type drop-down list only if Integrity client version 6.0 is installed on the endpoint computer.

The Zone Labs Cooperative Enforcement properties window appears.

4 In the Choose an EAP Type to Use for Authenticating the User dropdown list, do one of the following:

- Select **None**. Go to step 8.
- Select **Smart Card or other Certificate** and click **Properties**. Go to step 5.
- Select **Protected EAP (PEAP)** and click **Properties**. Go to step 6.

Do *not* choose **Secured Password** from the dropdown list, as that option is not supported. If you wish to use a secured password, choose **Protected EAP (PEAP)** and then, in step 6, select **Secured password** as the authentication method.

5 If you chose Smart Card or other Certificate, the Smart Card or Other Certificate Properties window appears.

In the When Connecting area of the properties window, make sure to *uncheck* the **Validate server certificate** checkbox. Then select **Use a certificate on this computer**. Go to step 8.

6 If you chose Protected EAP (PEAP), the Protected EAP Properties window appears. Do the following:

- In the When Connecting area, make sure to *uncheck* the **Validate server certificate** checkbox.

- In the Select Authentication Method dropdown list, choose the appropriate authentication method (**Secured password** or **Smart Card or other Certificate**) and click **Configure**.

The appropriate configuration dialog box appears.

7 Do one of the following:

- If you chose Secured password (EAP-MSCHAP v2), select the appropriate setting for **Automatically use my Windows login name and password...** (Generally, this checkbox should remain selected. If you do not plan to log in to the domain, however, uncheck this checkbox. This causes Integrity to prompt you for your domain credentials when you log in to the endpoint.)
- If you chose Smart Card or other Certificate, make sure to *uncheck* the **Validate server certificate** checkbox (in the When Connecting area), and then select **Use a certificate on this computer**.

8 Click **OK** in all relevant windows to save your changes and close the Network Connection manager.

The endpoint computer can now connect using Cooperative Enforcement.

Supported Enforcement Behaviors

When Cooperative Enforcement is configured, Integrity supports the following enforcement behaviors:

- VLAN switching
- filter enabling and disabling
- vendor-specific attributes (VSAs)
- reject the connection for non-compliance

Your particular gateway may not support all these enforcement options. For information about the options your gateway supports, see the vendor's product documentation.

Troubleshooting Your Installation

Use the tools described in this section to troubleshoot the components of your installation.

General

Use the `netsh` command to enable logging for the component you want. For gateway integration troubleshooting, the most useful logs are EAPOL, RASTLS, PPP, and RASEAP.

The command is: `netsh ras set tracing <component> enabled`

Internet Authentication Service

Use the Event Viewer to troubleshoot the Internet Authentication Service.

Integrity Advanced Server

Set the Integrity Server Logs in the XML file to **trace** to troubleshoot Integrity Advanced Server.

Integrity Client

Use the registry settings to troubleshoot the Integrity client.

To turn logging on in the registry (no restart necessary):

`hkey_local_machine\system\CurrentControlSet\Services\RasMan\PPP\EAP\255`

Setting	Meaning
Logging=0	Off (default)
Logging=1	Human readable
Logging=2	Human readable and binary

The log is stored in `Program Files\Zone Labs\Integrity Client\zlxeap.log`.

Network Access Server

For troubleshooting information about your NAS, see the configuration guide for that NAS.

Chapter 3

Nortel Contivity VPN Switch Integration

This chapter describes how to configure a Nortel Contivity™ VPN switch and Nortel Contivity clients to enable the Cooperative Enforcement feature.

The information provided here assumes that you have already installed and configured the Nortel Contivity VPN switch and client as well as the Contivity TunnelGuard Manager and Agent. For more information, see the Nortel Contivity installation guides.

This chapter assumes that you have performed the steps for configuring Cooperative Enforcement described in the *Integrity Advanced Server Administrator Guide*.

After installing and configuring Contivity and TunnelGuard, use the procedures in this chapter to configure the switch to interoperate with endpoint computers running Integrity client, and operating as VPN clients. Use bundled Java for TunnelGuard.

It is recommended that you install the Contivity client as an application.

To integrate Nortel Contivity VPN Switch with Integrity Advanced Server:

1. Configure the Nortel Contivity VPN Switch. (***See page 36.***)
2. Configure the Integrity clients. (***See page 49.***)

Configuring the Nortel Contivity VPN Switch

To configure the Nortel Contivity VPN Switch:

1 Enable the filters.

See "Enabling Tunnel Filter and Tunnel Management Filter," on page 36.

2 Create the software definition and TunnelGuard rule.

See "Creating an Integrity Client Software Definition and TunnelGuard Rule," on page 38.

3 Create a tunnel filter to the Integrity Server Sandbox.

See "Creating a Nortel Restricted Access Tunnel Filter to the Integrity Server Sandbox," on page 45.

4 Configure the tunnel filter and TunnelGuard rule.

See "Configuring the Restricted Access Tunnel Filter and the Integrity Client TunnelGuard Rule," on page 47.

Enabling Tunnel Filter and Tunnel Management Filter

Enable the Contivity Tunnel Filter and Contivity Tunnel Management Filter before creating a TunnelGuard filter rule that requires endpoint computers to have the Integrity client running.

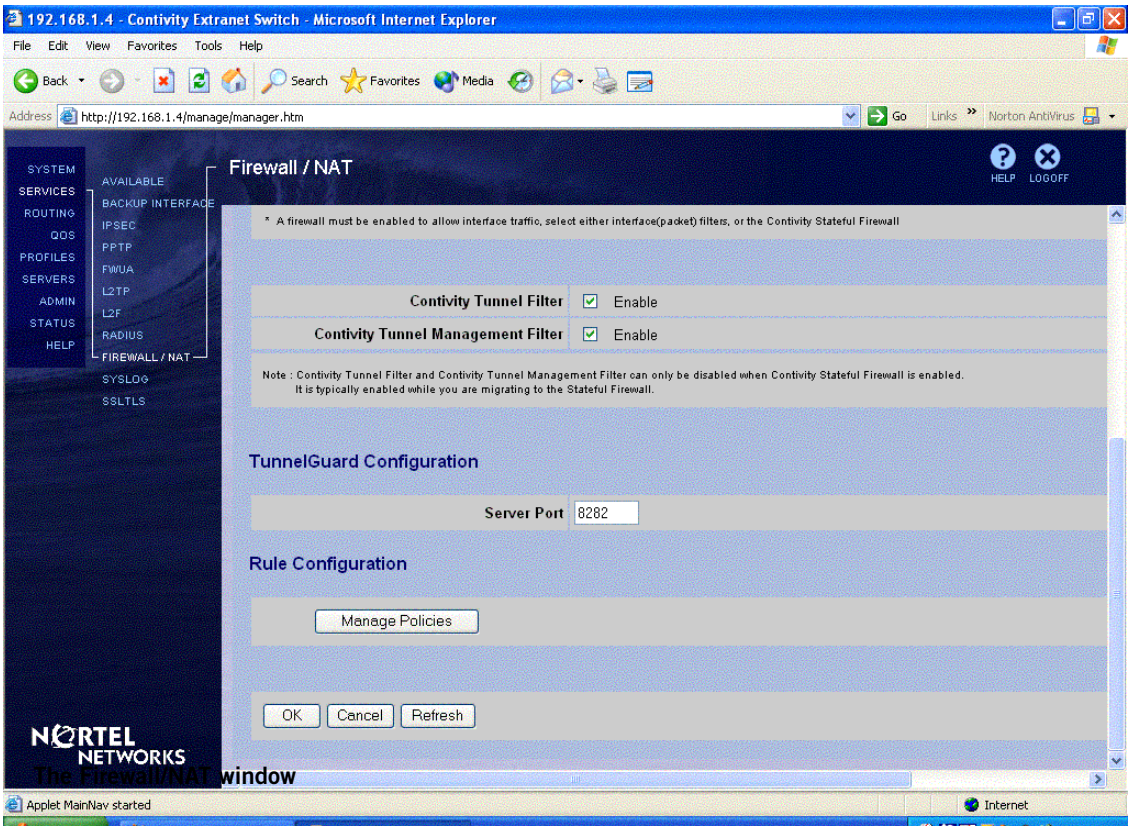
To enable Tunnel and Tunnel Management Filters:

1 Log in to the Nortel Contivity Switch Management Portal.

The Contivity Switch Management Portal Welcome page appears.

2 In the navigation pane at the left side, choose **Services** | **Firewall/NAT**.

The Firewall/NAT window appears.



The Firewall/NAT window

3 In the **Firewall/NAT** window:

a Scroll down until the two **Contivity** check boxes are visible.

b Select the **Contivity Tunnel Filter** check box.

c Select the **Contivity Tunnel Management Filter** check box.

d Click **OK**.

Tunnel Filtering is now enabled; continue with the next section to set up a filter on the gateway which allows endpoint computers running Integrity client to establish a VPN connection and access resources.

Creating an Integrity Client Software Definition and TunnelGuard Rule

After using the procedure in the preceding section to enable Contivity Tunnel Filter and Tunnel Management Filter, complete the following procedures to create an Integrity client Software Definition and TunnelGuard Rule.

To create the software definition and TunnelGuard rule:

1 Open the SRS Builder Utility Plug-in.

See “Opening the SRS Builder Utility Plug-in,” on page 38.

2 Create a new software definition and TunnelGuard Rule.

See “Creating a New Integrity Client Software Definition and TunnelGuard Rule,” on page 40.

3 Add the software definition to a TunnelGuard Rule.

See Adding the Integrity Client Software Definition to an Existing TunnelGuard Rule.

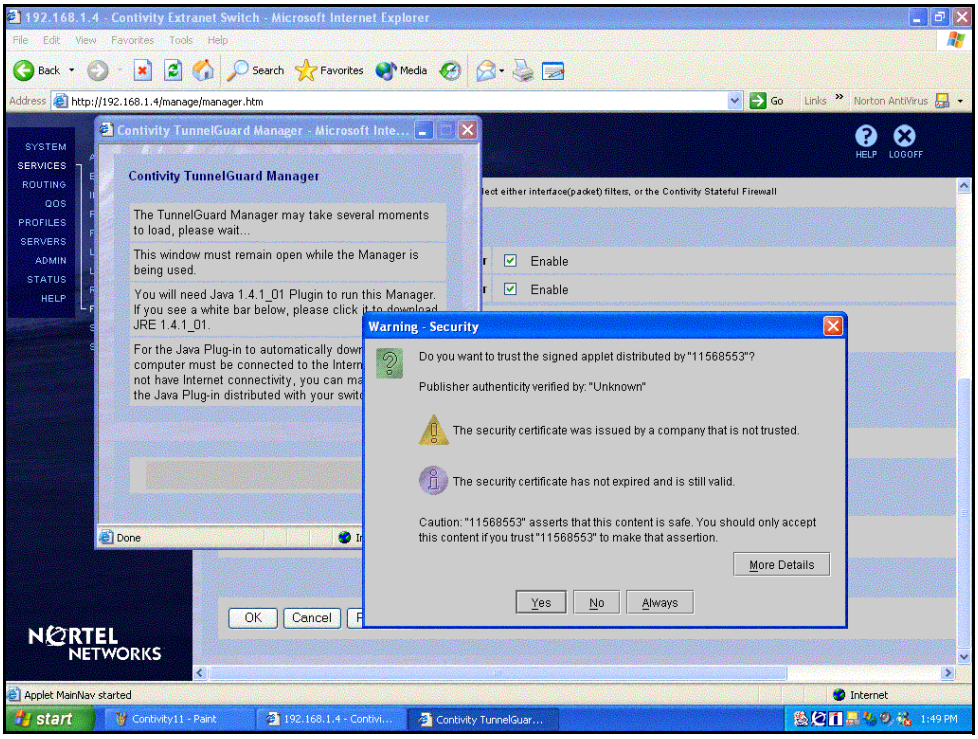
Opening the SRS Builder Utility Plug-in

The SRS Builder Utility Plug-in is a java applet that allows you to create and configure Software Definition and TunnelGuard Rules.

To open the SRS Builder Utility Plug-in:

1 Open the **Firewall/NAT** window, scroll further down until the **Contivity VPN Rule Configuration** area appears, then click **Contivity VPN Manage Policies**.

The Contivity Switch Management Portal displays the Java servlet notification dialog box.

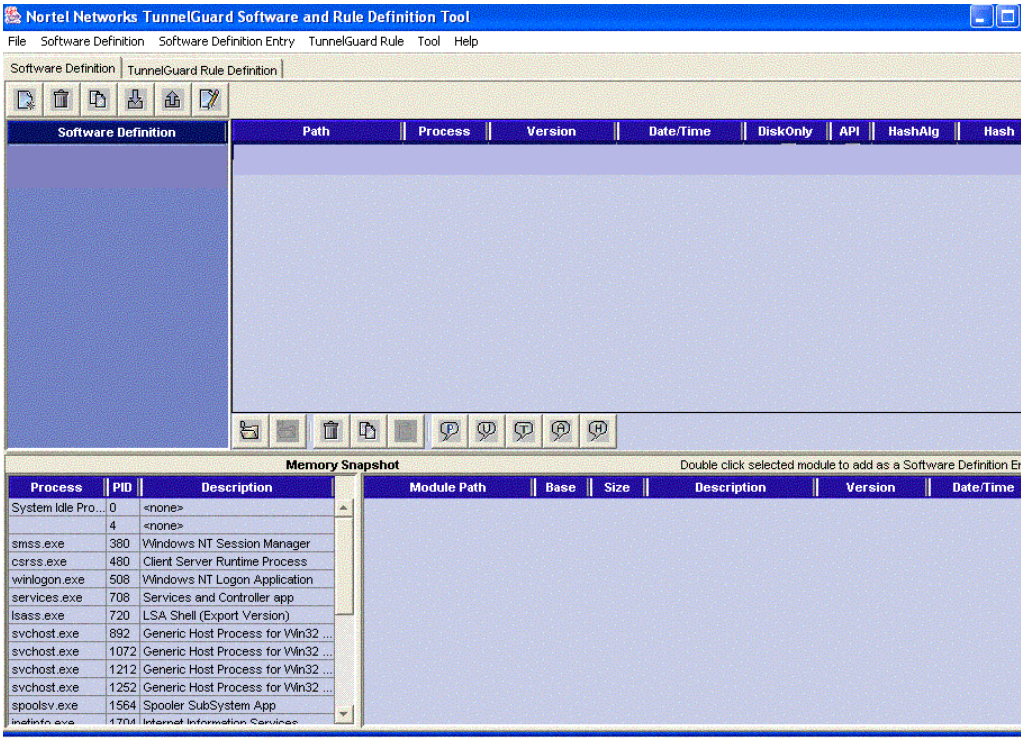


The Nortel Contivity Switch Management Portal, with Java download and certificate dialog boxes

The first time you use the Contivity VPN SRS Builder Utility Plug-in, a prompt to download and install the plug-in from the Internet appears. Follow the instructions provided by Nortel.

2 In the Java servlet dialog box, choose **Yes** to accept the applet's Contivity VPN security certificate or **Always** if you do not wish to receive this notice again.

The Contivity VPN SRS Builder Utility Plug-in takes a few moments to load. The Nortel Networks TunnelGuard Software and Rule Definition Tool window opens once the SRS update is complete.



The Nortel Networks TunnelGuard Software and Rule Definition Tool window

Creating a New Integrity Client Software Definition and TunnelGuard Rule

Create the Integrity client Software Definition and TunnelGuard Rule used by Cooperative Enforcement to ensure the security of the endpoint computer.

If you are using Integrity Flex and Integrity Agent clients on Windows 9x systems, you need to create an additional Software Definition and add it to the TunnelGuard Rule.

Create an Integrity client Software Definition and TunnelGuard Rule

If you are using Integrity Agent and Integrity Flex clients on Windows NT, 2000, or XP, and not Windows 9x, you only need to perform the steps in this section. If you also have clients, running Windows 9x, you must configure a Software Definition for those clients and add it to the TunnelGuard Rule.

To add an Integrity client Software Definition and TunnelGuard Rule:

1 Open the SRS Builder Utility Plug-in. In **Firewall/NAT** | **Rule Configuration**, click **Manage Policies**.

The SRS Policies are updated on your local machine from the Nortel Contivity VPN switch. After the SRS is updated, the **Nortel Networks TunnelGuard Software and Rule Definition Tool** window appears.

2 In the **Software Definition** tab, choose **Software Definition** | **Auto Generate TunnelGuard Rule**.

The Auto Generate TunnelGuard Rule is now selected.

3 Click the **New Software Definition** button.

The SRS Name dialog box appears.

4 In the **SRS Name** dialog box, type a name for the new rule (for example: Integrity client), then click **OK**.

The Software Definition is added to the list and a new TunnelGuard Rule with the same name is automatically created.

5 Add the Integrity client program file (vspubapi.dll) to the program file list. In the Software Definition list, select the Software Definition created in step **1**.

a Click on the **Add OnDisk File as Entry** (leftmost) button at the bottom of the program file list area.

The Open file dialog box appears.

b In the **Open** dialog box, browse to the Integrity client vspubapi.dll, then click **Open**.

For example, locate `c:\WINNT\system32\vspubapi.dll` on a computer that has the Integrity client installed, then click **Open**.

The vspubapi.dll is added to the Integrity client list of program files.

For endpoint computers that are configured differently, i.e., different drives or operating systems, redefine the path to the Integrity client program file using the Windows environment variable.

a In the file list area, select the Integrity client program file you just added.

b Click the **Custom Path** button.

The Custom Path dialog opens.

c Select the **Use Environment Variable** radio button, then enter path: **%WINDIR%\system32\vspubapi.dll**.

d Click **OK**.

The Integrity program file path appears as %WINDIR%\system32\vspuapi.dll.

6 Verify that the new rule has been created. In the **TunnelGuard Rule Definition** tab, a rule with the same name as the Software Definition you created in step **1** (for example: Integrity client) appears in the list of rules.

7 Save the software definition and rule. Choose **File** | **Save**.

If your endpoints running Windows NT, 2000 and/or XP only, this completes the creation of a TunnelGuard rule for Integrity client. Skip to "Adding the Integrity Client Software Definition to an Existing TunnelGuard Rule," on page 43.

If you have endpoints running Windows 98, continue to the next section.

Create an Integrity client Software Definition for Windows 9x Endpoints and Add it to the Integrity Client TunnelGuard Rule

If you have endpoints running Windows 9x, you must configure a Software Definition for the Windows 9x clients and add it to the TunnelGuard Rule.

To add an Integrity client Software Definition for Windows 9x endpoints:

1 Open the SRS Builder Utility Plug-in. In **Firewall/NAT** | **Rule Configuration**, click **Manage Policies**.

The SRS Policies are updated on your local machine from the Nortel Contivity VPN switch. After the SRS is updated, the **Nortel Networks TunnelGuard Software and Rule Definition Tool** window appears.

2 In the **Software Definition** tab, clear **Software Definition** | **Auto Generate TunnelGuard Rule**.

The Auto Generate TunnelGuard Rule is not selected.

3 Click the **New** button.

The SRS Name dialog box appears.

4 In the **SRS Name** dialog box, type a name for the new rule (for example: ZL- 9x), then click **OK**.

The Software Definition is added to the list and a new TunnelGuard Rule with the same name is automatically created.

5 Add the Integrity client program file (vspubapi.dll) to the program file list. In the Software Definition list, select the Software Definition created in step **1**.

a Click on the **Add OnDisk File as Entry** (leftmost) button at the bottom of the program file list area.

The Open file dialog box appears.

b In the **Open** dialog box, browse to the Integrity client vspubapi.dll, then click **Open**.

For example, locate `c:\Windows\system\vspubapi.dll` on a computer that has the Integrity client installed, then click **Open**.

The vspubapi.dll is added.

6 Enable the API for the Integrity client program file. In the bottom of the list of program files, click the **Add/Remove Vendor API Call Check** button.

The box in the API column of the definition appears selected.

7 Go to **TunnelGuard Rule Definition** tab, from the Available Expressions list select the rule you created in the previous section and the rule you created in this section.

Both rules move to the Group the list box.

8 Select **OR Expression**, then click **Form TunnelGuard Rule Expression**.

The rules are bound into a new expression (for example: *ZL-Integrity client or ZL-Integrity client 9x*) and appear in the Available Expressions box.

9 In the **TunnelGuard Rule Name** column, select the *Integrity Client TunnelGuard rule.*

10 In the TunnelGuard Rule Expression, select the expression you created in step 8 (ZL-Integrity client or ZL-Integrity client 9x).

11 Select **File** | **Save**.

This completes the creation of a TunnelGuard rule for Integrity client. Continue to the next section to configure the Nortel Contivity switch.

Adding the Integrity Client Software Definition to an Existing TunnelGuard Rule

Once an Integrity client software definition has been created, you can add it to an existing rule or rules. Only one TunnelGuard Rule can be configured per group. When you want to require several different programs, all software definitions must be in the same TunnelGuard Rule.

Groups on the Nortel Contivity VPN switch may already have an existing rule configured. Adding the Integrity client software definition to a configured rule will apply the Integrity client requirement without any additional steps.

To add the Integrity client software definition to an existing rule:

1 In the **TunnelGuard Rule Definition** tab, create an expression that includes all the software definitions you want in the rule.

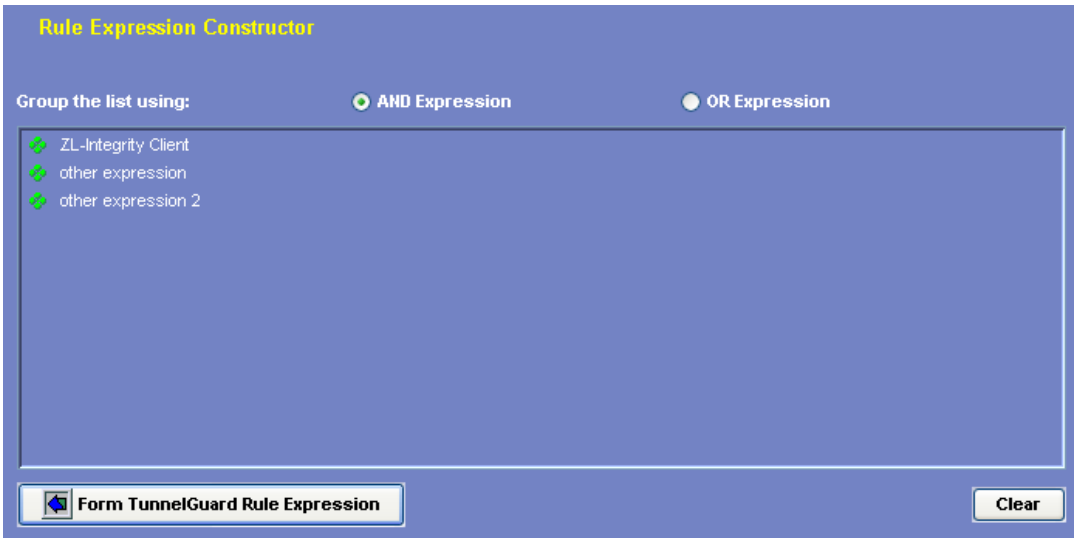
a Select the Integrity client software definition in the available expressions box, then click the **right-arrow** button to move it to the Rule Expression Constructor box.

For example: Integrity client is moved to the Rule Expression Constructor box.

b Select the other software definitions and/or existing expressions, then click the **right-arrow** button.

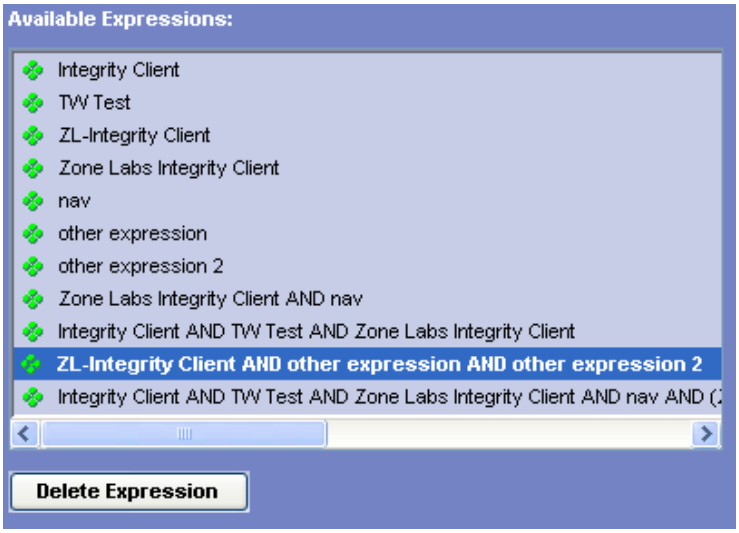
If you created an expression for Windows 9x, then select the expression ZL-Integrity Client or ZL-Integrity Client 9x and add it to the other conditions you want to apply.

All the expression are listed in the Rule Expression Constructor box.



c In Group the list using, select **And expression,** then click **Form TunnelGuard Expression.**

The new TunnelGuard Expression appears in the available expressions list. (For example: Integrity client AND *other expression* AND *other expression*.)



2 In the rule's TunnelGuard Expression drop-down list, select the expression you built in step **1**. (For example: select Integrity client AND other expression AND other expression.)

3 Save your changes to the rule. Choose **File** | **Save**.

The TunnelGuard Rule is added to the Nortel Contivity VPN switch.

4 Close the SRS Builder Utility Plug-in.

Creating a Nortel Restricted Access Tunnel Filter to the Integrity Server Sandbox

This section explains how to create a restricted access tunnel filter that allows endpoint computers that are out of compliance to access the Integrity Server sandbox and download the data they need to be compliant. Complete the following steps to allow access to the Integrity Sandbox:

To allow access to the Integrity Server Sandbox:

1 Create Access Rules for the Integrity Server Sandbox.

See "Create Access Rules for the Integrity Server Sandbox," on page 45.

2 Create a Restricted Access Tunnel Filter using the Integrity Server Sandbox Access Rules.

See "Create a Restricted Access Tunnel Filter using the Integrity Server Sandbox Access Rules," on page 46.

The Restricted Access Tunnel Filter created in this section is applied in the following section.

Create Access Rules for the Integrity Server Sandbox

Inbound and outbound access rules for the Integrity Server Sandbox are used to create the Restricted Access Tunnel Filter.

To create Integrity Server sandbox inbound and outbound rules:

1 Log in to the Nortel Contivity switch Management Portal, then choose **Profiles | Filters.**

The Filters dialog box appears.

2 In the **Current Contivity Tunnel Filters** box, choose **Manage Rules.**

The Tunnel Filters ->Manage Rules window opens.

3 Click **Create**.

The New Rule window opens.

4 Complete the new rule form as follows:

Field	Action
Rule Name	Enter a name for the rule (for example: IN_IntegritySandbox for the inbound rule and OUT_IntegritySandbox).
Filter Action	Select **Permit**.
Direction	Select **Inbound** or **Outbound**; create two rules, one for each direction of traffic.
Address	Choose the **Integrity Server IP address**; if the server is not listed click modify and add the Integrity Server.
Protocol	Select **TCP**.
Source Port	Select **GT or Equals** (Greater Than or Equals) and *any*, **0**.
Destination Port	Select **GT or Equals** and *any*, **0**.
TCP Connection	Select **Don't Care**.

5 Click **OK**.

The new rule appears in the Current Rules list.

6 Repeat steps 4 and 5 to create both an inbound and an outbound rule for Integrity Server.

7 Click **Close** to exit the Tunnel Rule Manager.

Create a Restricted Access Tunnel Filter using the Integrity Server Sandbox Access Rules

The Nortel Restricted Access Tunnel Filter is a rule set. Before creating the Filter, you must create inbound and outbound Integrity Server Sandbox rules.

To create a Restricted Access Tunnel Filter for the Integrity Server sandbox:

1 Create a new filter for the sandbox. In the Current Contivity Tunnel Filters, enter a name for the filter and click **Create**. (For example: ZL-Integrity Server Sandbox.)

The Tunnel Filter Set window opens.

2 In the **Available Rules** list, select the *Integrity Server inbound and outbound* access rules, then click the **left-arrow** button.

The selected rules are listed under Rules in set.

3 Click **OK** to save the Tunnel Filter set.

The Restricted Access Tunnel Filter appears in the Current Contivity Tunnel Filters.

Configuring the Restricted Access Tunnel Filter and the Integrity Client TunnelGuard Rule

The instructions in this section explain how to configure the Integrity client TunnelGuard rule created in "Creating an Integrity Client Software Definition and TunnelGuard Rule" section and the Integrity Server Sandbox Restricted Tunnel Filter created in "Creating a Nortel Restricted Access Tunnel Filter to the Integrity Server Sandbox" section to a group.

To configure the connection on the Nortel Contivity VPN Switch:

1 Log in to the Nortel Contivity switch Management Portal.

The Welcome window appears.

2 Select a group. In the Nortel Contivity VPN Switch's **Welcome** window, choose **Profiles | Groups**

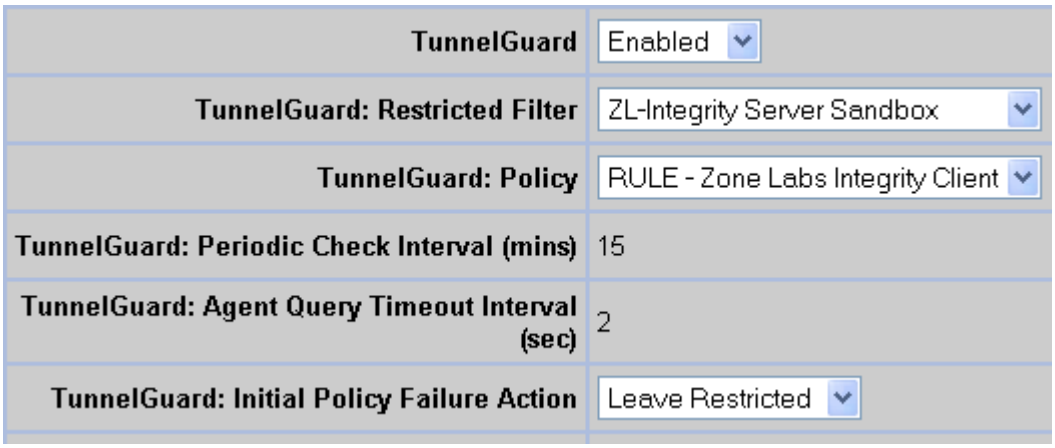
The Groups dialog box appears.

3 Edit the group to which you want to apply the Integrity client TunnelGuard Rule. In the Groups dialog box, click **Edit** next to the group.

Note: To create a new group, click **Add**, enter a name for the group, then click **OK.** When you create a new group, be sure to reconfigure all the attributes that you do not want inherited from the parent group.

4 Next modify the **TunnelGuard settings**. In the Connectivity box, choose **Configure**.

The Group's Connectivity Configuration window opens.



a Scroll down to the TunnelGuard options.

b If the group is configured to inherit these settings, you must click **Configure** to activate the drop-down list as shown above.

The following table shows the settings that are required to configure the Integrity Server and Integrity client on the Nortel Contivity VPN switch only.

Field	Action
TunnelGuard	Choose **Enable** from the drop-down list.
Contivity VPN TunnelGuard: Restricted Filter	Check Point recommends choosing the **Integrity Server sandbox rule** created in the previous section (for example: Integrity Server Sandbox) from the drop-down list.
TunnelGuard Policy	Choose the *Integrity Client TunnelGuard* rule created in the previous section
TunnelGuard: Initial Policy Failure Action	Choose **Leave Restricted**.

Additionally, put a copy of the Integrity client in the Integrity Server sandbox so that users with endpoint computers that are not in compliance with the TunnelGuard policy can update their computer and establish a connection.

c In the remaining TunnelGuard settings, choose the settings that are best suited for your network. Consult with your network administrator for details.

d Click **OK** to save and apply your changes.

The configuration is saved and applied to the group as well as any group which is a child configured to inherit TunnelGuard attributes.

5 Click **Logoff** to close the Nortel Contivity Management Portal.

The Integrity Server is configured on the Nortel Contivity VPN switch. To complete the Cooperative Enforcement feature, proceed to “Configuring the Integrity Clients,” on page 49.

Configuring the Integrity Clients

The Nortel Contivity VPN switch, Contivity TunnelGuard Manager and Contivity VPN client must be installed before you install Integrity clients on your endpoint computers. Refer to the Nortel Contivity installation guides for instructions on installing Nortel products.

To distribute Integrity Agent or Integrity Flex to your endpoint users, create client installation packages in Integrity Server and distribute links to them. For instructions, see the Integrity Installation and Configuration Guide.

When you create the installation packages to distribute your Integrity clients, be sure to add the IP address of the Contivity VPN Switch to the Trusted Zone in the default policy. This prevents the Integrity client from automatically blocking the connection to the Switch.

To configure the Integrity client:

1 Configure the baynet.tbk file.

See “Configuring the baynet.tbk File,” on page 49.

2 Configure the shortcut to iextranet.exe.

See “Configuring the Shortcut to iextranet.exe,” on page 50.

Configuring the baynet.tbk File

In order to integrate the Integrity Server with Nortel Contivity, you must modify the `baynet.tbk` file. After modifying the file, ensure that the updated `baynet.tbk` file is deployed with the VPN package to the endpoint computer. If you do *not* deploy the updated `baynet.tbk` file to the endpoint computer, end users will receive a prompt asking for the Integrity Advanced Server IP address. Deploying the `baynet.tbk` file prevents the possibility of end user error.

To configure the baynet.tbk file:

1 Open the `baynet.tbk` file.

2 Set `Server` to the gateway hostname or public IP address.

You may specify the Server using either the IP address or the DNS/hostname format, but it must be in the same format as the Nortel Public Host Name you gave for the gateway when you configured the Integrity Advanced Server. For more information, see the ***Administrator Guide***.

3 Set `IntegrityServer` to the Integrity Advanced Server IP address and port number: `1.1.1.1:443`.

Example:

```
[172.18.22.15]
```

```
Description=

Dialup=(None)

Username=newone

UseTokens=0

TokenType=0

UsePAPGroup=0

GroupName=

SavePassword=1

Server=172.18.22.15

primaryDNS=

secondaryDNS=

primaryWINS=

secondaryWINS=

domainName=

DisableKeepalive=0

EnableSilentKeepalive=0

IntegrityServer=172.18.1.31:443
```

4 Save the `baynet.tbk` file.

Configuring the Shortcut to iextranet.exe

When the installer for Integrity Flex or Integrity Agent runs, it detects the presence of the Nortel Contivity client on the endpoint and installs the file **iextranet.exe**. This application serves as a wrapper for the Integrity client and the Nortel Contivity client, enabling Cooperative Enforcement to function. A shortcut to the **iextranet.exe** application is placed on the desktop, with the label "Integrity Nortel VPN Client."

To connect to the Nortel VPN, with Cooperative Enforcement, the endpoint user must launch **iextranet.exe** by using this shortcut.

Integrity client installation does not remove pre-existing shortcuts to the Contivity client, which are similar in appearance to the Integrity Nortel VPN Client shortcut. If the user launches the VPN client using the old shortcut, Cooperative Enforcement will not operate properly. You may want to remove old shortcuts to avoid confusion. Alternatively, you can rename the extranet.exe and set the custom executable attribute to the new name. See "Setting the Custom Attribute," on page 51 for more information.

Option: No Desktop Shortcut

To prevent the shortcut to iextranet.exe from being placed on the desktop, include one of the following command line switches on the installer command line:

- For client version 4.5: **/nortel_noicon**
- For client versions 5.0 or later: **NORTELICON= NO**

Iextranet.exe and all other necessary files for Cooperative Enforcement are still installed.

Setting the Custom Attribute

To prevent users from avoiding cooperative enforcement by directly launching extranet.exe, rename extranet.exe on the end point computers and set the custom executable attribute in the tbk file.

To set the custom attribute:

1. Rename extranet.exe to <yourcustomname>.exe.
2. Open the baynet.tbk file and set the following attribute:

   CustomExecutable="C:\program files\nortel\<yourcustomname>.exe"

If you do not define a custom executable, iextranet.exe uses the extranet.exe as the default.

Chapter 4

Check Point Integration

This chapter describes how to integrate a Check Point Integrity client (Agent or Flex) with the Check Point Software Technologies VPN-1 SecureClient. Integration allows the Integrity client and SecureClient to coexist on endpoint computers and perform Cooperative Enforcement.

The information provided here assumes you have already installed FireWall-1 and VPN-1. For details about VPN-1/FireWall-1 installation, see Getting Started with Check Point Firewall-1.

This chapter also assumes you have performed the steps for configuring Cooperative Enforcement described in the Integrity Advanced Server Administrator Guide.

Cooperative Enforcement using SecureClient and SCV

You can use the Check Status model of Cooperative Enforcement to ensure that all endpoint computers logging in to your network using SecureClient are compliant with your security policies. For more information see the the Cooperative Enforcement chapter of the Integrity Advanced Server Administrator Guide.

SecureClient uses SCV checks to determine the overall security configuration of the computer. These security checks are performed at regular intervals, to ensure that only securely configured systems are allowed to connect and remain connected to the corporate VPN Gateway.

Each SCV check reports whether or not a security requirement has been satisfied. If any one of the requirements is not satisfied, the endpoint computer is disconnected or restricted, and the end user receives an error message.

See “Configuring the SCV Policy ,” on page 66 for more information about the requirements you can set in an SCV policy.

Cooperative Enforcement Workflow

The following describes the Cooperative Enforcement process using SecureClient.

1. SecureClient connects to the VPN-1 gateway.

   SecureClient initiates the connection to your system.

2. SecureClient connects to the Check Point policy server and receives the local.scv.

   The local.scv file (Secure Configuration Verification) contains the parameters you configure for the scan. See “Configuring the SCV Policy ,” on page 66 for more information.

3. The parameters are passed to the Zlscv.dll.

   The parameters contained in the local.scv file are passed by SecureClient to the Zlscv.dll.

4. The Zlscv.dll performs the check at the interval you set.

   The ZLscv.dll checks for compliance with all the parameters in the local.scv file and with the Integrity security policies. It scans for compliance at the frequency you set in the local.scv file and updates the global status accordingly. If the compliance check fails, the user receives a failure message, the event is logged, and the gateway is notified.

5. SecureClient checks the global status.

   SecureClient performs the global status check at the frequency you set on the checkpoint gateway, and permits, restricts, or denies access accordingly. The default frequency is 15 seconds.

Understanding the SecureClient/Integrity Client Unified Installer

The unified installer allows you to install SecureClient and Integrity Client along with the necessary policy file at the same time. See “Using Integrity SecureClient,” on page 57.

System Requirements

These requirements are in addition to the regular requirements for Integrity Advanced Server. For information about the system requirements, and supported versions, see the Integrity System Requirements Document.

- Check Point ® FireWall-1 NG with Application Intelligence R55W
- VPN-1® SecureClient™ with Application Intelligence R56
- A Check Point Integrity client version 6.0 or later
- Check Point Integrity Server version 6.0 or later
- Windows XP hotfix version Q329623 (unified installer only)

All Check Point software must include the latest HOTFIX updates.

Integrating Integrity Client with SecureClient

You can integrate an Integrity client with SecureClient in the following ways:

- Integrate with an existing SecureClient. See “Integrating with an Existing SecureClient,” on page 56.
- Integrate with an existing Integrity client. See “Integrating with an Existing Integrity Client,” on page 56.
- Use Integrity SecureClient. This combined product installs both the Integrity client and SecureClient from one installation file. Use this option when neither SecureClient nor Integrity client exists on the endpoint computer. See “Using Integrity SecureClient,” on page 57.

Integrating with an Existing SecureClient

Use this integration method when a configured Check Point SecureClient already exists on the endpoint computer, and you are now installing an Integrity client.

To integrate with an Existing SecureClient:

1. Configure your VPN-1/FireWall-1 installation. See “Configuring your VPN-1/Firewall-1 Installation,” on page 60.
2. Configure the SecureClient. See “Configuring the SecureClient Installation,” on page 64.
3. Check that the computer is securely configured. See “Checking that the Computer is Securely Configured,” on page 65.
4. Install an Integrity client with your existing SecureClient. See “Installing an Integrity Client after SecureClient,” on page 65.
5. Check the connection. See “Checking the Connection,” on page 66.
6. Configure the SCV policy. See “Configuring the SCV Policy ,” on page 66.
7. Install the new SCV policy. See “Installing the SCV Policy on Policy Servers,” on page 69.
8. Configure the Integrity client for use with SecureClient. See “Configuring an Integrity Client for Use with SecureClient,” on page 71.
   a. Observe the SecureClient programs using Integrity Server.
   b. Configure an enterprise policy.
9. Create an installation package. See “Packaging the Policy File,” on page 74.

Integrating with an Existing Integrity Client

Use this integration method when an Integrity client already exists on the endpoint computer, and you are now installing a Check Point SecureClient.

To integrate with an existing Integrity client:

1. Configure your VPN-1/FireWall-1 installation. See “Configuring your VPN-1/Firewall-1 Installation,” on page 60.
2. Install the Check Point SecureClient. See “Installing SecureClient after Integrity Client,” on page 65.
3. Configure the SecureClient. See “Configuring the SecureClient Installation,” on page 64.
4. Check that the computer is securely configured. See “Checking that the Computer is Securely Configured,” on page 65.
5. Check the connection. See “Checking the Connection,” on page 66.
6. Configure the SCV policy. See “Configuring the SCV Policy ,” on page 66.
7. Install the new SCV policy. See “Installing the SCV Policy on Policy Servers,” on page 69.
8. Configure the Integrity client for use with SecureClient. See “Configuring an Integrity Client for Use with SecureClient,” on page 71.
   a. Observe the SecureClient programs using Integrity Server.
   b. Configure an enterprise policy.
9. Deploy the enterprise policy. See the Chapter 2 of the Integrity Administrator Guide, “Policy Studio Overview,” for more information about deploying an enterprise policy.

Using Integrity SecureClient

Use Integrity SecureClient when neither Integrity client nor SecureClient is already installed on the endpoint computer. The combined product installation package installs both clients. You can either use either of the following options:

- The prepackaged Integrity SecureClient package (Recommended)

  See “Using the prepackaged Integrity SecureClient package,” on page 57.

- A custom unified installation package

  See “Using a custom unified installation package,” on page 59.

Using the prepackaged Integrity SecureClient package

A prepackaged Integrity SecureClient package is provided on the Check Point Webpage. Use the prepackaged Integrity SecureClient package to get a standard installation without having to configure the clients to work together.

To use the prepackaged Integrity SecureClient package:

1 Obtain and unzip the IntegritySecureClient_X_X_XXX_<language>.zip file from the Check Point Website.

The zip file contains the following files:

- sc_iflex_client.exe—The package file for SecureClient with Integrity Flex
- sc_ia_client.exe—The package file for SecureClient with Integrity Agent
- hostconfig.bat—A configuration batch file that allows you to specify the IP address of the Integrity Advanced Server.
- hostconfig.vbs—A configuration script that allows you to specify several parameters.
- hostconfig_readme.txt—The readme for the configuration script

2 Use the configuration scripts to create the configuration file.

You can use either the hostconfig.bat (recommended) or the hostconfig.vbs. Use the hostconfig.bat if you only want to specify the Integrity Advanced Server IP address. Use the hostconfig.vbs to specify other parameters.

To use the hostconfig.bat:

Open a command script window and type the following, specifying the host:

hostconfig.bat <host>

Argument	Type	Description
<host:443/cm>	Required	The IP address of the Integrity Advanced Server

The hostconfig.vbs file must be located in the same directory as hostconfig.bat.

Use hostconfig.bat only for endpoint users that connects through NT Domain and when Integrity Advanced Server is configured to use the NT Domain catalog. Using any other catalog, for example, Custom, Gateway, IP catalog, LDAP, or RADIUS will result in the endpoint receiving the default policy instead of the assigned enterprise policy.

To use the hostconfig.vbs:

Open a command script window and type the following using the appropriate argument(s):

cscript //nologo hostconfig.vbs -h <host> -p <port> -t <trigger> -n <name> -d <delaytime>

Argument	Type	Description
-h <host>	Required	The IP address of the Integrity Advanced Server
-p <port>	Optional	The Integrity Advanced Server port number (defaults to “6054”)
-t <trigger>	Optional	The trigger mechanism (defaults to “Always”)
-n <name>	Optional	The name of the connection (defaults to “Integrity Server”
-d <delaytime>	Optional	The delay time for the connection (defaults to “-1”

3 Use a third party application to distribute the appropriate executable to your endpoint computers.

4 If you are upgrading the Integrity SecureClient, note that it does not retain the previously configured settings.

After upgrading, perform the following steps:

a Double click the SecureClient icon in the system tray.

A dialog window appears asking you to set up the new site. Click **Yes** to continue.

b Enter the VPN-1 server address and click **Next**.

c Select **Certificate** and click **Next**.

d Click **Browse...**, select the file with the .p12 extension and click **Open**.

e Enter your CP VPN server password and click **Next**.

f Select Advanced and click **Next**.

g Select Visitor Mode, and click **Next**.

SecureClient will attempt to validate your certificate. Once the certificate is authenticated, click **Next**.

h Click **Finish**.

Integrity SecureClient is now installed on your endpoint computers. You may skip the rest of this chapter.

Using a custom unified installation package

If you need to configure your clients, you will need to create a custom unified package.

To integrate using a custom unified installation package:

1 Configure your VPN-1/FireWall-1 installation. See “Configuring your VPN-1/Firewall-1 Installation,” on page 60.

2 Configure the SCV policy. See “Configuring the SCV Policy ,” on page 66.

3 Install the new SCV policy. See “Installing the SCV Policy on Policy Servers,” on page 69.

4 Configure the Integrity client for use with SecureClient. See “Configuring an Integrity Client for Use with SecureClient,” on page 71.

   a Observe the SecureClient programs using Integrity Server.

   b Configure an enterprise policy.

5 Create a unified installation package. See “Packaging the Policy File,” on page 74.

Integrity SecureClient uses Integrity client version 5.0 or later; you cannot downgrade the Integrity client portion independently after installing Integrity SecureClient. Doing so may cause SecureClient errors.

Creating a localized unified installation package

Use the following steps to create a unified installation package for a language other than English.

To create a localized unified installation package:

1 Obtain a localized SecureClient executable.

   See the Check Point documentation for more information about obtaining a localized SecureClient executable.

2 Follow the instructions in “Packaging the Policy File,” on page 74 to create the unified installation package.

   a In the Product Information area, include the localized SecureClient executable.

   b In the Product Information area, include the localized Integrity client executable.

Configuring your VPN-1/Firewall-1 Installation

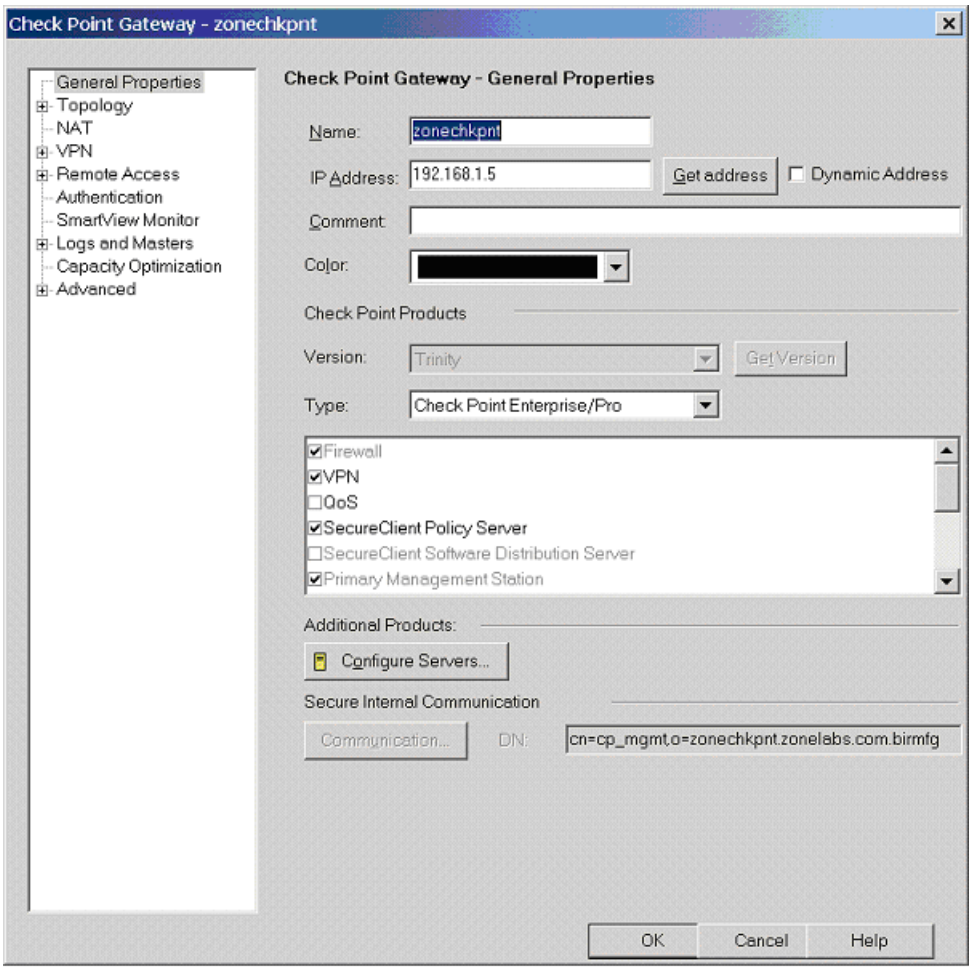
Perform the following steps to enable your VPN-1/FireWall-1 installation to work with Checkpoint Integrity client.

If you are using the NGX R60 version of VPN-1, refer to your VPN-1 documentation for configuration information.

To configure your VPN-1/Firewall-1 installation:

1 In the *Check Point SmartDashboard* window, select **Network Objects** | **Check Point** then right-click your firewall and choose **Edit**.

The General Properties window appears.



2 Select the **SecureClient Policy Server** check box.

This enables the SecureClient policy server on the VPN-1/Firewall-1 gateway.

3 Configure the firewall installation as specified in the Check Point documentation.

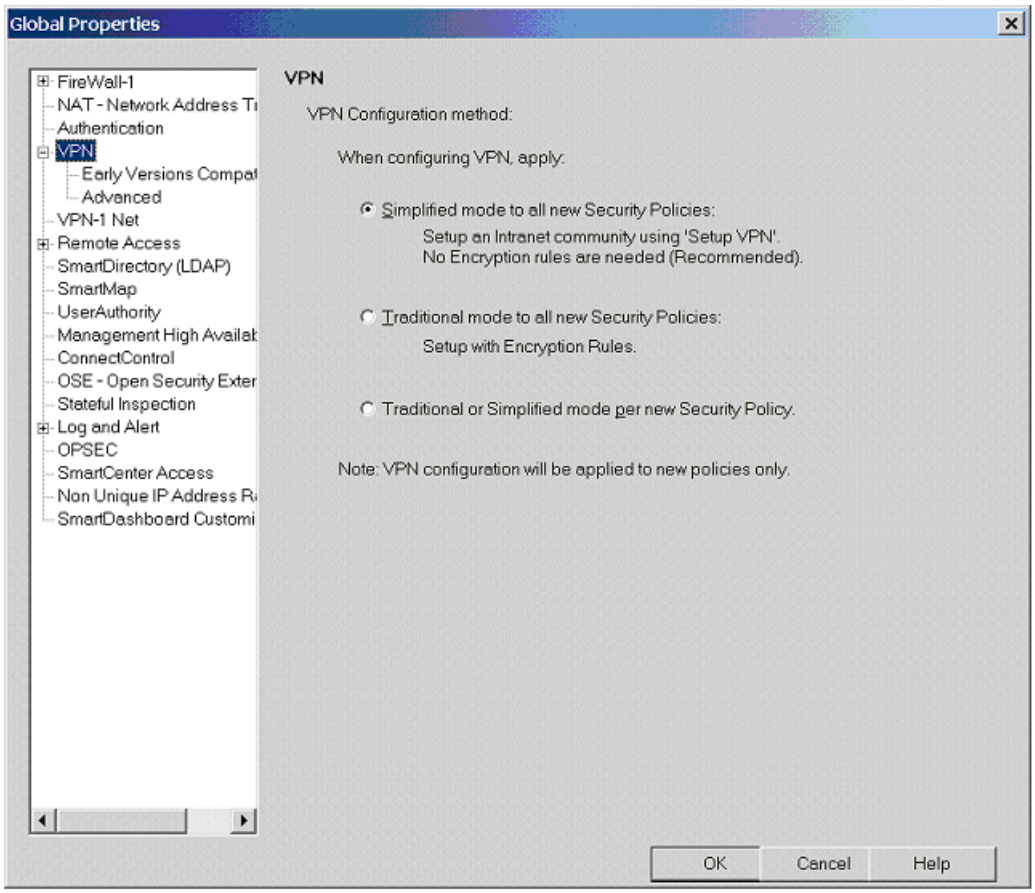
These steps include:

- Defining the Topology
- Defining Authentication
- Defining a Policy Server User
- Giving a User Group Firewall Access
- Define Desktop Security Rules

- Defining Policies

4 Select **Policy** | **Global Properties** | **VPN**.

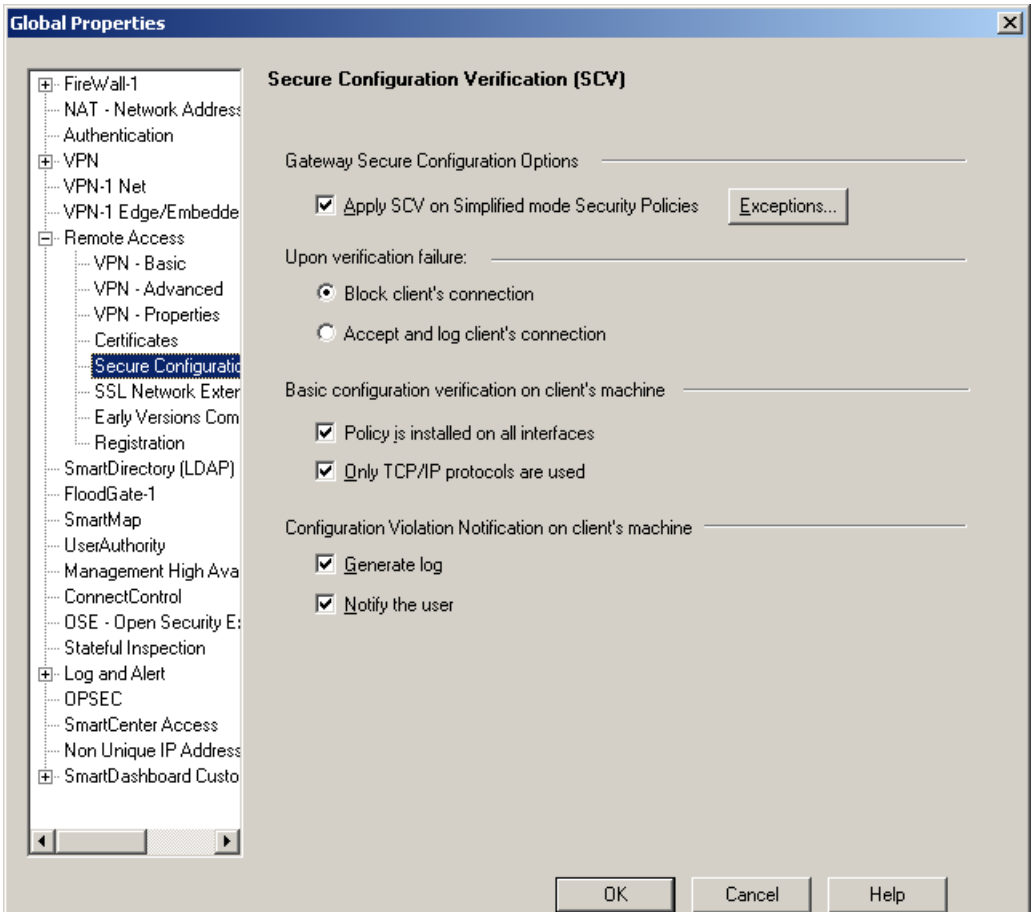
The Global Properties VPN window appears.



5 Select the **Simplified mode to all new Security Policies** radio button.

6 Select **Remote Access** | **Secure Configuration Verification (SCV)**.

The Secure Configuration Verification (SCV) window appears.



7 Select the **Apply Secure Configuration Verifications on Simplified mode Security Policies** check box.

8 if you want to restrict new connections when SCV fails, select the **Block client's connection** check box. If you want to allow new connections when SCV fails, select the **Accept and log client's connection** check box.

9 Set the Services.

If you selected **Block client's connection** in step 8, you must set services for HTTP without SCV, HTTPS without SCV service, and for the Zone Security Protocol 2 so they can bypass the SCV check.

a Go to **Services** and right click **Other**.

b Choose **New Other...**

c Type the **Name** and **Description** for the HTTP without SCV service.

d Set the **IP Protocol** to 6.

e Click **Advanced**.

f In the **Match** field, set the dport to the destination port on which the service is running and set SCV to not verify.

dport=<destination port>, r_scvres=SCV_DONT_VERIFY

g Click **OK**.

h Click **OK**.

i Repeat steps a-g for HTTPS without SCV service and the Zone Security Protocol 2.

For Zone Security Protocol 2 set the IP Protocol to 17 and dport to 6054.

10 If you selected **Block client's connection** in step 8, you must create firewall rules for the services you defined in step 9.

In order to allow the Integrity client to communicate with Integrity Server, create firewall rules accepting the services. For example:

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
npool	lateday	Any Traffic	HTTPS_wo_SCV	accept	Log	Policy Targets	Any
npool	lateday	Any Traffic	HTTP_wo_SCV	accept	Log	Policy Targets	Any
npool	lateday	Any Traffic	ZSP2	accept	Log	Policy Targets	Any

For more information on creating firewall rules, see your Check Point documentation.

If the Integrity Server is behind the gateway the VPN address must not be in NAT format.

11 Select **Policy** | **Install** and click **OK**.

The policy deploys.

Configuring the SecureClient Installation

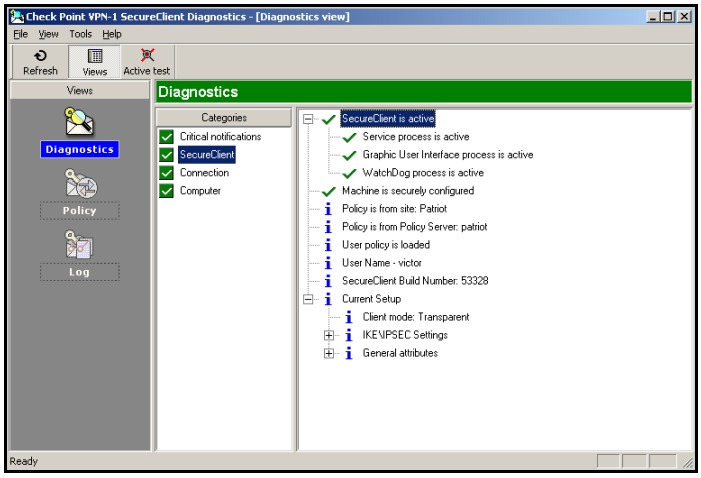
Configure the SecureClient as described in the Check Point documentation.

Checking that the Computer is Securely Configured

To check that the computer is securely configured:

1 Launch SecureClient Diagnostics.

The *Check Point VPN-1 SecureClient Diagnostics* window appears.



The Check Point VPN-1 SecureClient Diagnostics window

2 Verify that the **Machine is Securely Configured** check mark is green.

If your computer is not securely configured refer to Check Point documentation in order to resolve the problem.

3 Close SecureClient Diagnostics.

Installing an Integrity Client after SecureClient

Install an Integrity client by running the Integrity client installer, and proceed through the installation screens.

The Integrity client installation restarts your SecureClient. Therefore, expect to lose your VPN connection. After the installation, you must re-enter your credentials.

Installing SecureClient after Integrity Client

If you install Integrity client on a computer which does not have a Check Point Secure Client, the Integrity client installer installs all the files necessary for later integration, but does not configure Integrity client for SCV checks. After installing the Check Point secure client, you must manually run the Check Point SCV Plug-In installer in order to configure Integrity client for Check Point SCV checks.

To install Check Point SecureClient after an Integrity client:

1. Perform the Check Point SecureClient installation as described in the Check Point documentation.
2. Browse to the Zone Labs directory.
3. Run the Check Point SCV Plug-In installer file (zlscvins.exe).

The Check Point plugin installation restarts your SecureClient. Therefore, you lose your VPN connection. After the installation, you must re-enter your credentials.

Checking the Connection

Perform the following steps to check the connection to the Integrity client.

To check the connection:

1. Access the errorlog.txt file in the c:winnt\internet directory.
2. Check the log for the message “The registration of the zlscv.dll was successful”.

Configuring the SCV Policy

Configure your SCV (Secure Configuration Verification) policy. When endpoint computers connect to your network, SecureClient downloads the policy file (local.scv) and runs the SCV check to ensure that the endpoint computer is securely configured. The SCV check is repeated at intervals defined in the policy itself.

The SCV check will fail under the following conditions:

- There is no SCV policy (local.scv file) on the computer. This will occur if the endpoint user never logged on to a Policy Server, or if the file was erased.
- The local.scv file is either corrupted or not configured correctly. If SecureClient is configured to revert to a backup copy of local.scv and the local.bak file is corrupted as well, the computer is not securely configured.
- One or more of the checks that are enabled in the SCV policy reported failure.
- The endpoint user selected either Disable Policy from the Policy menu or Delete from the Site menu.
- The SCV policy has timed out, and the endpoint user has not logged on to a policy server.
- One or more SCV checks specified by the SCV policy are missing or not configured correctly on the endpoint computer.

To configure the SCV policy file:

1. With a text editor, open $FWDIR\conf\local.scv on the Smart Center (management) server. This may be the same server as your enforcement server. You can also use

the SCV Editor available from Check Point to edit the SCV file. See “Sample Configured SCV Policy,” on page 68.

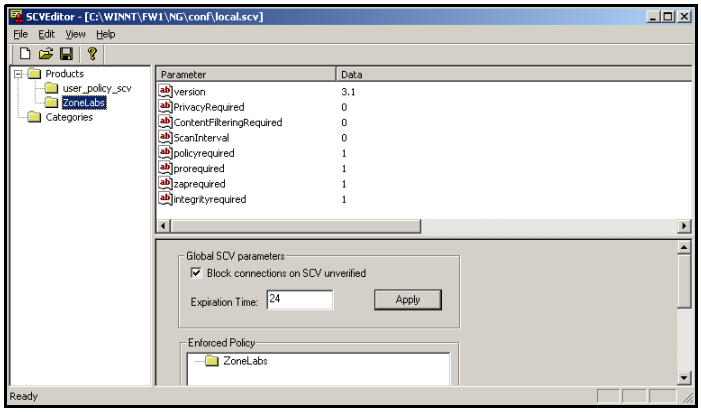
2 Insert the appropriate Check Point SCV policy parameters into the SCVNames section of the file. See “Check Point SCV Policy Parameters,” on page 67, for policy parameter definitions.

The Check Point SCV plugin name is ZoneLabs.

The SCVEditor

Check Point provides a tool for editing SCV files. You can download it from www.checkpoint.com. For information about how to use SCVEditor and local.scv, refer to Check Point documentation.

Be sure to select Enforce from the Zone Labs directory item, on the left side of the SCV Editor window. This enforces the running of the corresponding SCV dll on the endpoint computer.



The SCV Editor window

Check Point SCV Policy Parameters

The following parameters are defined for the Check Point SCV plug-in. If you omit a parameter, the scan will use the default value.

Parameter	Description	Default
ScanInterval	Specifies the number of seconds between scans. If you set this parameter to 0, the scan is not repeated. The minimum interval between scans is 5 seconds.	60
Version	Specifies the minimum version for the Integrity client. Endpoint computers with an older version will fail the SCV check.	4.0.0

Parameter	Description	Default
PolicyRequired	Set this parameter to 1 if you want to require that the endpoint computer have a policy. Set it to 0 to not require a policy.	0
IntegrityServer	Location of the Integrity Server, formatted as IP:port number.	None
ContentFilteringRequired	Set this parameter to 1 to require that content filtering be turned on. Set it to 0 to not require content filtering.	0
IntegrityRequired	Set this parameter to 1 if you want to require users to have Integrity Flex or Integrity Agent, rather than Integrity Desktop. Set this parameter to 0 if you want to allow users with Integrity Desktop access to your system.	0
ProRequired	Set this parameter to 1 if you want to require users to have Integrity Flex or Integrity Desktop rather than Integrity Agent. Set this parameter to 0 if you want to allow users with Integrity Agent to have access to your system.	0
ZAPRequired	Set this parameter to 1 if you want to require users to have Zone Alarm Pro. Set this parameter to 0 to not require Zone Alarm Pro.	0
PrivacyRequired	Set this parameter to 1 if you want to require users to have the Privacy feature enabled. Set this parameter to 0 to not require the Privacy feature.	0

Sample Configured SCV Policy

This example shows a configured local.scv file.

```
: (ZoneLabs
        :type (plugin)
   :parameters (
     :ScanInterval (60)
     :Version ("5.0")
     :IntegrityRequired (1)
     :PRORequired (0)
     :ZAPRequired (0)
     :PrivacyRequired (0)
     :ContentFilteringRequired (0)
     :PolicyRequired (1)
     :IntegrityServer ("172.18.1.31:443")
   )
)
```

```
        )
        :SCVPolicy (
         : (ProcessMonitor)
         : (ZoneLabs)
        )
        :SCVGlobalParams (
         :enable_status_notifications (true)
         :status_notifications_timeout (10)
         :disconnect_when_not_verified (false)
         :block_connections_on_unverified (false)
         :block_scv_client_connections (false)
         :scv_policy_timeout_hours (168)
         :enforce_ip_forwarding (false)
         :not_verified_script ("")
         :not_verified_script_run_show (false)
         :not_verified_script_run_admin (false)
         :not_verified_script_run_always (false)
         :allow_non_scv_clients (false)
        )
)
```

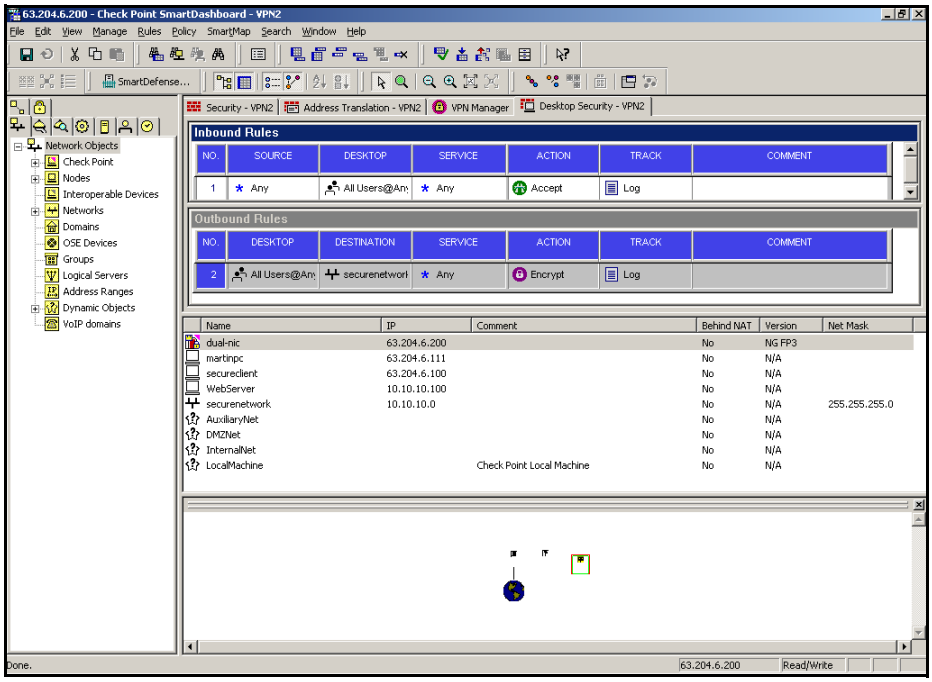
Installing the SCV Policy on Policy Servers

After creating your Check Point SCV policy, you must install it on the Policy Servers on your network. Once installed on the servers, the policy is downloaded and implemented by SecureClients.

To install the new SCV policy on Policy Servers:

1 Launch the Check Point SmartDashboard.

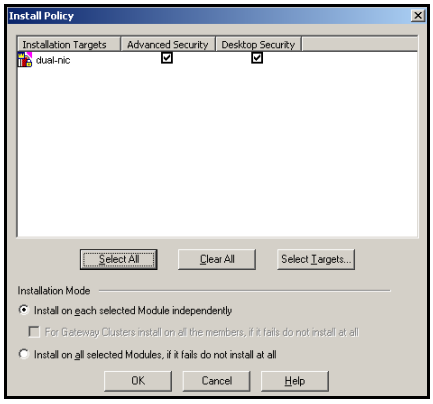
The *Check Point SmartDashboard* window appears.



The Check Point SmartDashboard window

2 Select Install from the Policy menu at the top of the window.

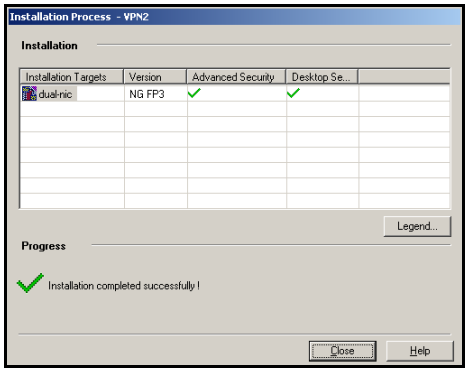
The *Install Policy* window appears.



The Install Policy window

3 Install the policy as necessary, to Security and/or Desktop Security, and click **OK**.

The *Installation Process* window appears.



The Installation Process window

4 Verify that the policy installs correctly via the installation process window and click **Close**.

The *Check Point SmartDashboard* window returns.

When the endpoint user logs in and authenticates on VPN-1 SecurRemote/ SecureClient, The SCV Plug-In automatically reads the relevant configuration information into memory from the Check Point VPN Gateway located in the local.scv file.

Troubleshooting the Check Point SCV Configuration

If the SCV Plug-In encounters an improperly formatted line in local.scv, the default Zone Labs parameters settings will be restored and the following entry appears in the SecureClient log:

Zone Labs SCV Plug-In encountered an input error restoring default parameters.

If you encounter this error message, do the following:

1 Edit the local.scv file and fix the necessary line(s).

2 Reinstall the policy.

3 Reconnect via SecureClient.

Configuring an Integrity Client for Use with SecureClient

To configure Integrity Agent or Integrity Flex for use with Check Point SecureClient, the SecureClient executables need to be given network access permission in the Check Point Integrity security policy. You will first run SecureClient on a secure computer that is already connected to Integrity Server, in order to allow the program observation feature to capture the Smart Checksums of the SecureClient executables. You will then create an enterprise policy giving the proper permissions to those executables. In the

same policy, you must add your Check Point VPN, your Office Mode IP addresses and all gateway and policy servers to the Trusted Zone to allow SecureClient to communicate with your VPN servers.

To configure your Integrity client:

1 Observe the SecureClient programs using Integrity Server. See page 72.

2 Configure an enterprise policy. See page 73.

Required Rules Summary

If you already know how to configure an Integrity enterprise policy with program rules, use the table as a guide to creating the needed rules and then add the Check Point VPN to the Trusted Zone. Otherwise, see below for detailed instructions.

Program Rules

Application	Act as Client (Trusted)	Act as Client (Internet)	Act as Server (Trusted)	Act as Server (Internet)
SR_SERVICE.EXE	Allow	Allow	Allow	Block
SR_GUI.EXE	Allow	Allow	Allow	Block
SCC.EXE	Allow	Allow	Allow	Block
SR_SDS.EXE	Allow	Allow	Block	Block
SR_DIAGNOSTICS.EXE	Allow	Allow	Block	Block

Trusted Zone Definition

- Add your Check Point VPN to the Trusted Zone.

Observing the SecureClient Programs Using Integrity Server

Install Integrity Agent or Flex and SecureClient on a secure computer and then use the Integrity Server to observe the SecureClient executables.

To observe the SecureClient Programs

1 Install SecureClient on a secure computer.

2 Deploy an Integrity client installer package to the same secure computer, and install and launch the Integrity client (Integrity Agent or Integrity Flex). The Integrity client will automatically download and implement the default policy or an assigned policy from Integrity Server when it is launched.

3 Set program observation.

a In the Integrity Server Administrator Console, open the Program Rules panel.

b Select the **Record program activity** check box and set the **Observation period** to 120.

c Click the Client Settings tab.

d Set the **Heartbeat frequency** and the **Log transfer frequency** to **High**.

4 Deploy the policy.

If your default policy is already in use by a large number of clients, you may not want to enable program observation in the default policy, as this may greatly increase bandwidth and database use. If this is the case, consider assigning a discovery mode policy to the secure reference computer.

5 On the secure computer, launch SecureClient, to enable Integrity to observe the executables. The executables appear in the Integrity Server Program Manager, and can be added to policies.

6 Right-click on the SecureClient icon and choose **Launch SecureClient Diagnostics**.

7 For CLI users: connect using the SCC command line.

8 Software Distribution Service users should launch the Software Distribution Agent.

Configure the Enterprise Policy

Be sure

When you have finished observing the executables, be sure to turn off program observation.

Use Integrity Server to create a policy that allows each SecureClient to communicate with the VPN server.

To configure the enterprise policy:

1 In Integrity Server, create a policy giving the required permissions to the SecureClient executables.

a In the Integrity Administration page, navigate to **Policy Studio** | **Policy List**.

b Choose your policy from the list and click **Edit**.

c Click the **Program Rules** tab.

d Click **Add**.

e Click **All Programs**.

f Select the following programs from the list and then click **Add**:

- SR_SERVICE.EXE
- SR_GUI.EXE
- SCC.EXE
- SR_SDS.EXE

- SR_DIAGNOSTICS.EXE

The executables you observe will depend on which version of SecureClient you have installed. You may not observe all the executables listed above.

g Select or deselect the check boxes for **Allow Internet** and **Allow Trusted** as specified in "Program Rules," on page 72.

2 Add your Check Point VPN to the Trusted Zone.

a Click the **Access Zones** tab.

b Click **Add**.

c Choose **Adding a new Source/Destination** from the drop down list.

d Complete the fields with the information for your Check Point VPN servers. You may need to add more than one entry if you have multiple servers.

e Click **Add**.

3 Repeat step 2 for the Office Mode IP addresses and all gateway and policy servers.

Packaging the Policy File

Now that you have configured your policy, you can add that policy to an Integrity Flex or Integrity Agent installation package. When SecureClient users install an Integrity client, the policy will automatically allow SecureClient to connect to your Check Point VPN.

Before including the policy in an Integrity Flex installer package, make sure "Enforce enterprise policies only" is selected in the Client Settings tab of the policy.

To package the configuration file with Integrity Flex or Integrity Agent:

1 In the directory for the installer package with which you want to bundle the policy, create a directory called **extras**. For example:

c:\Program Files\Zone Labs\Integrity\jakarta-tomcat-4.0.1\webapps\integrity\package\Integrity_Flex_US_5_0_556_026\extras

2 From Integrity Server, export the enterprise policy you just created to the **extras** directory.

a Go to **Policy Studio** | **Main Page**.

b Select the policy you just created.

c Click **Export: XML format**.

d Click **Save** and navigate to the **extras** directory you just created, and save the file as CPpolicy.xml

3 In Integrity Advanced Server, go to **Client Functions | Client Packager**.

4 Click **New**.

5 In the **Package Details** area, enter the name for the new package.

6 In the **Product Information** area, enter the package information:

   a Select the type of Integrity client.

   b Select an Integrity client installer file.

   c Enter the product version number.

   d Select **Add SecureClient installer file to package** and specify the SecureClient installer file.

7 In the **Install Parameters** area, enter the appropriate information:

   a In the **Install Directory,** enter the location where you want the clients installed.

   b In the **Additional Parameters** field, enter the following:
   POLICYFILE="$temp$\CPPolicy.xml"

8 Complete the rest of the New Package screen per your own requirements.

9 Click **Save** to save the installation package.

   You can now distribute the new installation package normally.

For additional information on using installation packages, see the Integrity Installation and Configuration Guide.

Chapter 5

Cisco VPN 3000 Series Concentrator Integration

This chapter describes how to configure the Cisco VPN Series Concentrator (Cisco Concentrator) to enable the Cooperative Enforcement feature.

The information provided here assumes that you have already installed and configured the Cisco VPN 3000 Series Concentrator. For more information, see the Cisco Concentrator installation guides.

This chapter also assumes that you have performed the steps for configuring Cooperative Enforcement described in the Integrity Advanced Server Administrator Guide.

This document contains the following sections:

System Requirements

These are the general components you will need to use the Cisco Concentrator with Integrity Advanced Server. For more detailed system requirements and version information, see the Integrity Advanced Server System Requirements document.

- Check Point Integrity Server
- An Integrity client
- Cisco VPN 3000 Series Concentrator
- Cisco VPN client

You can use either the Cisco clustering option or the Integrity Advanced Server clustering option, but not both.

Integrating Cisco VPN 3000 Series Concentrator with Integrity

Perform the following steps to integrate your Cisco Concentrator with the Integrity Server.

To integrate the Cisco Concentrator:

1 Configure the Cisco Concentrator.

See "Integrating Cisco VPN 3000 Series Concentrator with Integrity," on page 78.

2 Configure client enforcement.

See "Configuring Client Enforcement," on page 79.

Configuring the Cisco Concentrator

Configure the Cisco Concentrator with the connection information for the Integrity Server.

To configure the Cisco Concentrator:

1 Set the Firewall.

See "Setting the Firewall," on page 78.

2 Configure Client Enforcement

See "Configuring Client Enforcement," on page 79.

Setting the Firewall

Set the firewall in the Cisco Concentrator to Zone Labs Integrity Server.

To set the firewall:

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate to **Configuration** | **System** | **Servers** | **Firewall.**

2 In the **Zone Labs Integrity Server** field, enter the IP address for your Integrity Server.

If you are using clustering, enter the IP address of the firewall or load balancer.

If you later change this IP, traffic will still be routed to the Integrity Advanced Server until you remove the Cisco gateway from Integrity Advanced Server.

3 Set the **Failure Policy** options as appropriate for your installation.

4 In the **Server Port** field, enter the port for your Integrity Server. The default value is 5055.

This value cannot be 5054 and must match the port value in “Checking Port Settings,” on page 88.

5 Choose whether or not to use a SSL certificate to authenticate the Integrity Server.

Note

If you select the **SSL Client Authentication** check box, you must import a SSL Certificate into the Integrity Server from the Cisco Concentrator before Cooperative Enforcement will occur. Be sure to use the appropriate key for the Concentrator interface. Use the Certificate Manager panel in the Integrity Server to import the certificate.

Configuring Client Enforcement

Configure the Cisco Concentrator to require that connecting endpoint computers have an Integrity client installed. Configure client enforcement by performing the following steps.

1 Create a group on the Cisco Concentrator.

See “Creating a group,” on page 79.

2 Set the firewall policy.

See “Setting the firewall policy,” on page 80.

Creating a group

If you have not already created a group, do so now. If you have already created a group, edit it as appropriate.

To create a group:

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate to **Configuration** | **User Management** | **Groups.**

2 Click **Add Group**.

3 Click the **Identity** tab.

4 In the **Group Name** field, enter name for the group. You must use the same name you used for the gateway group on the Integrity Server.

5 Complete the other fields and click **Add**.

Setting the firewall policy

To set the firewall policy

1 Click the **Client FW** tab.

The VPN Client Firewall Policy page opens.

2 Select the **Firewall Required** radio button in the **Firewall Setting** field.

3 In the **Firewall** drop-down list, select **Zone Labs Integrity**.

4 Complete the other fields and click **Add**.

Configuring the Integrity Client

Configure the Integrity client to allow the Cisco VPN Client to communicate with the Cisco Concentrator.

If your endpoint computers are using Integrity Agent, you can use the Integrity Server to configure Integrity Agent through the enterprise policy. If your endpoint computers are using Integrity Flex, you will have configure both the enterprise policy, using the Integrity Server, and the personal policy. If your endpoint computers are using Integrity Agent and you have customized the personal policy, you will also need to configure the personal policy.

Overview of client communications

Cisco VPN on the endpoint computers, communicate with the Integrity Server in the following way:

1. A Cisco VPN client contacts the Cisco Concentrator.
2. The Cisco Concentrator performs initial authentication of the user.
3. If authentication is successful, the tunnel is placed into a restricted state, only allowing network connectivity to the Integrity Server.
4. The Integrity client sends the Cisco gateway group name and user name to Integrity Server.
5. If the Integrity Server is unreachable, the Cisco VPN reverts to AYT (Are You There) functionality. The Concentrator will then contact the Cisco VPN client and will verify if the Integrity client service is running. If the Integrity client service is running then the VPN user will be allowed VPN access to the network.
6. The Integrity client sends a synchronize request to the server. The Integrity Server performs a lookup for the gateway group that matches the VPN group. It then selects the appropriate policy based on this information. The location of the policy to download and other information is sent back to the Integrity client.
7. If the Integrity client does not have the policy it downloads it. It then sends another synchronize call to the server and reports compliance. the connection is removed for restricted mode. If the second synchronize call does not arrive within six heartbeats, the Integrity Advanced Server tells the VPN gateway to terminate the connection.
8. Once connected, the Integrity client cannot be closed without also terminating the VPN connection. The VPN client hooks directly into the Integrity firewall service and will not allow it to be terminated. If the service is terminated through extraordinary means, the VPN connection will be immediately closed.
9. By default, if the Integrity client misses four consecutive heartbeats, the connection is restricted. If the Integrity client misses six subsequent heartbeats, the VPN tunnel is torn down and the connection is terminated. You can set the frequency of

heartbeats, and the number of heartbeats before termination or restriction in the Client Settings for a policy.

Perform the following steps to configure your Integrity client so that the Cisco VPN client can connect to the VPN Gateway:

To configure the Integrity Client:

1 Configure the Enterprise Policy.

See "Configuring the Enterprise Policy," on page 82.

2 Package the Policy file for Integrity Flex or Agent.

See "Packaging the Policy File with Integrity Flex or Agent," on page 85.

Configuring the Enterprise Policy

Configure the enterprise policy to allow the Cisco VPN client to establish a VPN connection. If your endpoint computers are using Integrity Agent, you can use the Integrity Server to configure the Integrity Client through the enterprise policy. If your endpoint computers are using Integrity Flex you will also have to configure the personal policy. If your endpoint computer are using Integrity Agent and you have configured the personal policy, you will also need to include the policy file in an Integrity Flex or Integrity Agent installation package.

To configure the enterprise policy:

1 Add the Cisco Concentrator access Zone.

See "Adding the Cisco Concentrator Access Zone," on page 82.

2 Add the localhost access Zone.

See "Adding the Localhost Access Zone," on page 83.

3 Add the LAN access Zone.

See "Adding the LAN Access Zone," on page 83.

4 Add the program rules.

See "Adding the Program Rules," on page 84.

5 Turn off policy arbitration.

See "Turn off Policy Arbitration," on page 84.

Adding the Cisco Concentrator Access Zone

To Add the Cisco Concentrator access Zone

1 In the Integrity Administrator Console, go to to **Policy Studio** | **Policies**.

2 Choose your policy from the list and click **Edit**. If you haven't already created a policy for the gateway defined group for the cisco Concentrator, do so now.

3 Click the **Access Zones** tab.

4 Click **Add**.

5 Choose **Include the network in the Trusted Zone**.

6 Click **New Location**.

7 Complete the fields according to the table below.

Field	Value
Type	IP Address
Name	Cisco Concentrator
Host	<public IP address of your Concentrator>

8 Repeat steps 6 and 7 for each gateway and click **Save**.

Adding the Localhost Access Zone

To Add the localhost access zone

1 In the Access Zones page, click **New Location**..

2 Complete the fields according to the table below.

Field	Value
Type	IP Address
Name	localhost
Host	127.0.0/1

3 Click **Save**.

Adding the LAN Access Zone

To add the LAN access zone:

1 In the Access Zones page, click **New Location**.

2 Complete the fields according to the table below.

Field	Value
Type	Subnet
Name	LAN
Host	<your network address and subnet mask>

3 Click **Save**.

Adding the Program Rules

Set the program access rules to allow the VPN client to communicate with the Cisco Concentrator.

To add the program access rules:

1 In the Integrity Administration page, navigate to **Policy Studio** | **Policy List**.

2 Choose your policy from the list and click **Edit**.

3 Click the **Program Rules** tab.

4 Click **Add**.

5 Click **All Programs**.

6 Select the following programs from the list and then click **Add**:

- CVPND.EXE
- IPSECDIALER.EXE
- IPSXAUTH.EXE
- VPNGUI.EXE
- PPPTOOL.EXE

The executables you see here depend on the version you are using.

7 Select the check boxes for **Allow Internet** and **Allow Trusted** for both client and server settings.

Turn off Policy Arbitration

To ensure that the personal policy does not block the VPN communication, turn off policy arbitration.

To turn off policy arbitration:

1 Go to Policy **Studio** | **Policies**.

2 Select your policy and click **Edit**.

3 Click the Client Settings tab.

4 Select the **Enforce enterprise policies only** check box.

Packaging the Policy File with Integrity Flex or Agent

Now that you have configured your policy, you can add that policy to an Integrity Flex or Integrity Agent installation package. When users install Integrity Flex, the policy will automatically allow your endpoints to make a VPN connection.

To package the configuration file with Integrity Flex or Integrity Agent:

1 In the directory for the installer package with which you want to bundle the policy, manually create a directory called **extras**. For example:

```
c:\Program Files\Zone Labs\Integrity\jakarta-tomcat-
4.0.1\webapps\integrity\package\Integrity_Flex_US_5_0_556_026\extras
```

2 From Integrity Server, export the enterprise policy you just created to the **extras** directory, saving it as CCpolicy.xml.

   a Go to **Policy Studio** | **Main Page**.

   b Select the policy you just created.

   c Click **Export**.

   d Navigate to the extras directory you just created, and save the file as CCpolicy.xml

3 In Integrity Server, go to **Configuration** | **Client Deployment**.

4 Click select the installation package you want to use, then click **Edit**.

5 Under Install Parameters, in the **Additional Parameters** box, add the following:

   - For Integrity versions earlier than 5.0:

```
/policy “$temp$\extras\CCPolicy.xml”
```

   - For Integrity version 5.0 or later:

```
POLICYFILE= “$temp$\extras\CCPolicy.xml”
```

6 Complete the rest of the Edit Package screen per your own requirements.

7 Click **Save** to save the installation package.

   You can now distribute the new installation package normally.

For additional information on using installation packages, see the Integrity Installation and Configuration Guide.

Troubleshooting

If you experience difficulties with your installation, perform the following checks.

To troubleshoot the connection between the servers:

1 Check the connection to the Integrity Server.

See “Checking connection to the Integrity Server,” on page 86.

2 Check the logs.

See “Checking the Log files,” on page 86.

3 Check the SSL certificate exchange.

See “Checking the SSL Certificate Exchange,” on page 87.

4 Check the validity of the SSL certificate.

See “Checking the SSL Certificate Validity,” on page 87.

5 Check the encryption type.

See “Creating a new Secure Socket Layer Certificate,” on page 88.

6 Check the port settings on the Cisco Concentrator.

See “Checking Port Settings,” on page 88.

Checking connection to the Integrity Server

Verify that the Cisco Concentrator can connect to the Integrity Server.

To check the connection to the Integrity Server

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate to **Administration** | **Ping.**

2 In the **Address/Hostname to Ping** field, enter your Integrity Server IP address.

If your ping is successful you will be informed that your Integrity Server IP address is ‘alive’. This means that the Cisco Concentrator is able to connect to the Integrity server and you can proceed.

If your ping is not successful, you should check to make sure that traffic can pass between the two servers and that the settings you used when configuring the Cisco Concentrator and the Integrity Server are correct. If the settings are all correct, proceed to try the other troubleshooting procedures in this section.

Checking the Log files

You can use either the Integrity Server log or the Cisco Concentrator log to confirm that the two devices are communicating.

The Integrity Server Log

The Integrity Server log file is located at: `C:\Program Files\Zone Labs\Integrity\jakarta-tomcat-4.0.1\webapps\integrity\logs`

The file is called integrity.log and can be opened in any text editor. Set the logging level to high. If the server and Concentrator are not communicating you will see an error message immediately after adding the Concentrator. The log will also indicate a successful connection.

The Concentrator log

The Concentrator live event log shows if communications have failed. Top view the live event log, navigate to **Monitoring** | **Filterable Event Log** | **Live Event Log**. If you see entries resembling the following, you must create a new Secure Socket Layer Certificate:

08/02/2002 11:53:13.140 SEV=4 IKE/159 RPT=1

TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access

See "Creating a new Secure Socket Layer Certificate," on page 88 for more information.

Checking the SSL Certificate Exchange

The SSL certificate is exchanged between the Cisco Concentrator and the Integrity Server via HTTP. Check that HTTP is enabled on the Cisco Concentrator.

To verify that HTTP is enabled:

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate to **Configurations** | **System** | **Management Protocols** | **HTTP/HTTPS**.

2 Verify that **Enable HTTP** is checked and that the **HTTP Port** matches the certificate port that you specified for the gateway device in Integrity Server.

Checking the SSL Certificate Validity

Check to make sure the SSL Certificate is still valid.

To check the SSL Certificate validity:

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate to **Administration** | **Certificate Management**.

The Certificate Management page opens.

2 Find the SSL Certificate in the list of SSL certificates and click **View**.

3 Check the validity field to see if the certificate has expired and if it matches the Integrity Server SSL Certificate.

If the certificate has expired, or does not match, you will need to create a new one. See "Creating a new Secure Socket Layer Certificate," on page 88 for instructions on how to create a new certificate.

Creating a new Secure Socket Layer Certificate

Perform the following steps to create a new SSL Certificate when needed.

To create a new Secure Socket Layer Certificate:

1 Delete the Concentrator entry from Integrity Server.

2 Delete all SSL certificates from the gateway device.

3 Generate a SSL certificate on the Concentrator.

The Cisco Concentrator and the Integrity server will exchange new certificates automatically.

4 Create a Concentrator entry within Integrity Server to the internal interface on the VPN server.

5 Verify the SSL certificate has been exchanged by editing the gateway entity on the Integrity Advanced Server.

You do not need to change any settings to cause a new certificate exchange to take place. Make sure that the SSL certificate download port on the Cisco Concentrator is not blocked.

Checking the Encryption Type

Check that the encryption types for the two servers do not match.

To check the encryption type:

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate to **Configuration** | **Tunneling and Security** | **SSL** | **Protocols**.

2 Check that the **SSL Version** is set to Negotiate SSL V3/TLS V1.

Checking Port Settings

Integrity Server and the Integrity clients use the Zone Labs Security Protocol (ZSP). Check to make sure that Cisco Concentrator is not blocking the traffic on this port.

To check the port:

1 Open the Cisco VPN 3000 Concentrator Series administrative console and navigate **Configuration** | **Policy Management** | **Traffic Management** | **Rules.**

2 Check that the rules do not prevent ZSP traffic from passing through the Cisco Concentrator. ZSP uses port 5055 by default. This value must match the value you used when setting the firewall, see “Setting the Firewall,” on page 78.

Chapter 6

InterSpect Gateway Integration

This chapter describes how to configure Check Point InterSpect™ internal security gateways ("InterSpect") and Integrity Advanced Server to provide intra-LAN Cooperative Enforcement.

The information provided here assumes that you have already installed and configured the InterSpect Gateway. For more information about InterSpect, refer to the User Guide that is provided with the InterSpect product or available for download as a PDF from the Check Point Web site.

Configure InterSpect *before* you configure Integrity Advanced Server for Cooperative Enforcement. For more information about the order of configuration, see the chapter on Cooperative Enforcement in the *Integrity Advanced Server Administrator Guide*.

The following topics are covered:

Benefits of InterSpect integration

Unlike VPN gateway products, the InterSpect internal security gateway provides security inside the network. InterSpect complements perimeter gateway devices, allowing the network administrator to provide security on the basis of software defined Intra-network zones such as LAN segments.

Integrating InterSpect with Integrity Advanced Server provides the benefits of Cooperative Enforcement to computers that connect to the network from inside the firewall or VPN gateway perimeter.

System Requirements

These are the general components you will need to integrate your Check Point Interspect gateway with Integrity Advanced Server. For more specific system requirements and version information, see the Integrity Advanced Server System Requirements document.

- Check Point Integrity Advanced Server
- An Integrity client
- Check Point InterSpect gateway
- Check Point InterSpect SmartDashboard for SmartCenter Server, version 2.0 or later

For more information about InterSpect, see the ***Check Point InterSpect*** user manual.

Configuring the InterSpect gateway

This section lists tasks required to configure InterSpect for Cooperative Enforcement.

To configure the InterSpect gateway:

1 "Verify that the gateway is set to bridge mode," in the following section

2 "Create an Integrity Server Intra-network zone," on page 93

3 "Set up the bridge configuration," on page 94

4 "Set up Integrity Advanced Server general properties," on page 95

Verify that the gateway is set to bridge mode

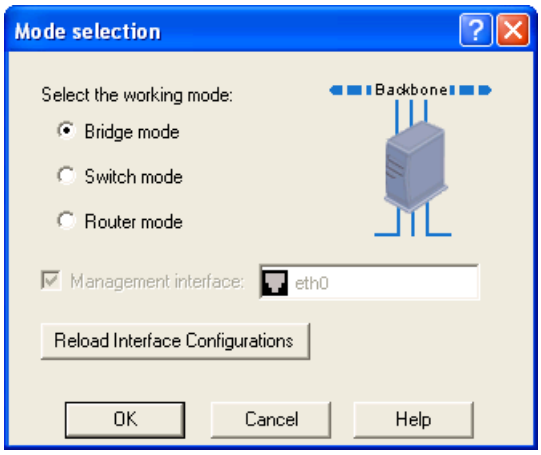
The InterSpect gateway operates in bridge mode by default. Verify that the gateway is in bridge mode before configuring an Integrity Advanced Server connection.

To verify the gateway mode:

1 Open the Check Point InterSpect SmartDashboard.

2 Click the **Overview** tab, then click **Mode selection**.

The Mode Selection dialog box appears.



3 Select **Bridge mode.**

4 Click **OK**.

Create an Integrity Server Intra-network zone

On the Segmentation panel, the Zone pane contains icons representing currently defined Intra-network zones. If you already created an Integrity Server Intra-network zone, select the Integrity Server zone and go to "Set up the bridge configuration," on page 94.

To create a new Intra-network zone:

1 In the Check Point InterSpect SmartDashboard, select the **Segmentation** tab.

2 In the **zone pane**, right-click then choose **New**.

A new zone form appears in the main pane to the right.

3 In the **Name** area, type the name of the new zone.

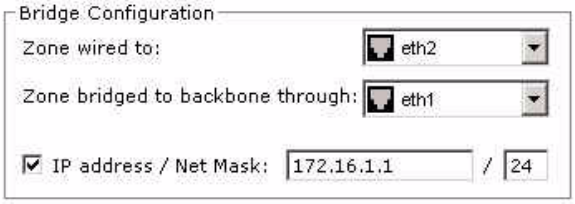
Set up the bridge configuration

Set up the LAN segment, LAN backbone, and quarantined page access.

To set up the bridge configuration:

1 Go to **Bridge Configuration** on the Segmentation tab.

Verify that the Integrity Intra-network zone is selected in the zone pane.



2 Select the LAN segment to protect from the **Zone wired to** drop-down list.

3 Select the LAN backbone in the **Zone bridged to backbone through** drop-down list.

4 Optionally, select **IP address/Net Mask**, then type the IP address and subnet mask.

This address is used to serve the quarantined page. It must be accessible by client computers in the wired zone.

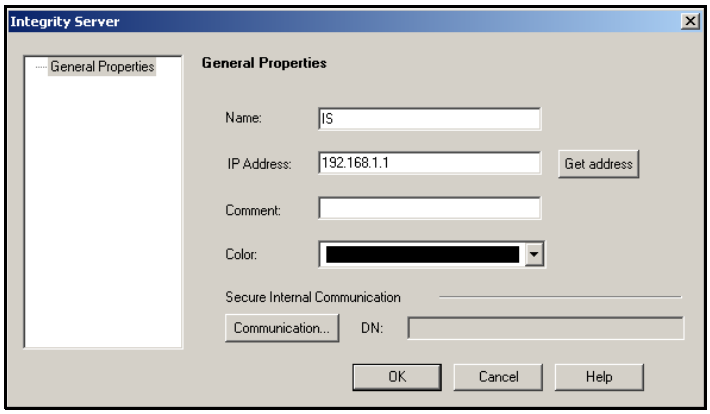
Set up Integrity Advanced Server general properties

Configure InterSpect to use Integrity Advanced Server.

To configure InterSpect to use Integrity Advanced Server:

1 In the Integrity Configuration area, select **Use Integrity Server**.

The Integrity Server configuration dialog box appears.



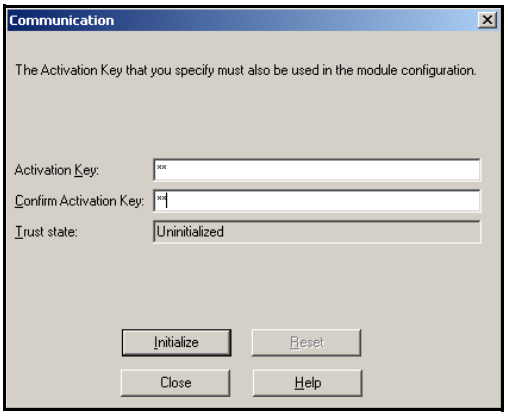
2 In **Name**, type the Integrity Advanced Server host name.

Make note of the name, because you must use it as the ***SIC Object Name*** when creating the corresponding gateway catalog on Integrity Advanced Server.

3 In **IP Address**, type the Integrity Advanced Server IP address.

4 Click **Communication** to set the activation key.

The Communication dialog box appears.



a In **Activation Key**, type the authentication code used to secure the communication between the InterSpect gateway and Integrity Advanced Server.

Make note of the key, because you must enter it in the ***SIC Activation Key*** field when creating the corresponding gateway catalog on Integrity Advanced Server.

b Re-enter the key in **Confirm Activation Key**.

c Click **Initialize** to save your changes.

The following message appears in the Trust State field: "Initialized but trust not established." (This is expected. Trust is established only later, after you configure the corresponding gateway catalog on Integrity Advanced Server.)

d Click **Close**.

5 Click **OK** to save your changes and return to the Segmentation window.

Configure connections *to* the zone

Decide how to handle traffic that is connecting through the gateway to the Integrity protected zone.

To configure connections to the zone:

1 In the Connections To Zone area, select **Authorize using Integrity Server**.

2 Click **Configure** to set the gateway actions for various traffic conditions.

The Integrity Server Action Properties window appears.

a Select the desired action (Inspect, Bypass, Block, Quarantine) and tracking level (None, Log, Alert, Mail, SNMP Trap, or user-defined) for the various conditions. (For descriptions of these action and tracking options, see the *Check Point InterSpect* user manual.)

For example, an administrator might configure InterSpect to quarantine hosts that have been refused authorization or that have no Integrity client, and to block connections when Integrity has not sent a response or when it is not connected.

b Click **OK**.

3 Perform the following steps to allow clients to get an IP address.

Clients must have IP addresses to communicate with the Integrity Advanced Server.

a In the Connections to Zone area, click **Exceptions**.

The Exceptions to Zone Settings dialog box appears.

b Add entries for ports 53 (DNS), 67 (DHCP), and 68 (DHCP) to the list of exceptions. For each entry:

- Click **Add**.
- Type the port number.

- Set the Protocol, Action, and Track options as desired.
- Click **OK**.

Configure connections *from* the zone

To prevent authorized computers from sending traffic outside the network through the gateway, use Integrity Advanced Server to protect outbound traffic as well.

To configure connections from the zone:

1 In the **Connections From Zone** area, select **Authorize using Integrity Server**.

2 Click **Configure** to set the gateway actions for various traffic conditions.

The Integrity Server Action Properties window appears.

a Select the desired action (Inspect, Bypass, Block, Quarantine) and tracking level (None, Log, Alert, Mail, SNMP Trap, or user-defined) for the various conditions. (For descriptions of these action and tracking options, see the *Check Point InterSpect* user manual.)

For example, an administrator might configure InterSpect to quarantine hosts that have been refused authorization or that have no Integrity client, and to block connections when Integrity has not sent a response or when it is not connected.

b Click **OK**.

3 Perform the following steps to allow clients to get an IP address.

Clients must have IP addresses to communicate with the Integrity Advanced Server.

a In the Connections to Zone area, click **Exceptions**.

The Exceptions to Zone Settings dialog box appears.

b Add entries for ports 53 (DNS), 67 (DHCP), and 68 (DHCP) to the list of exceptions. For each entry:

- Click **Add**.
- Type the port number.
- Set the Protocol, Action, and Track options as desired.
- Click **OK**.

Apply the settings to gateway traffic

To enforce your settings on traffic coming through the gateway, do the following:

On the toolbar, click **Activate Settings**. Then click **Yes | Close**.

Configuring Integrity Advanced Server

On the Integrity Advanced Server, do the following:

- Configure a gateway catalog for the InterSpect gateway.
- Configure an IP catalog that includes the IP addresses of all endpoint computers (with Integrity clients) that you want the gateway to monitor.

- Create a policy to assign to endpoints that the gateway will monitor. The policy should include access zones that mirror the zones established on the InterSpect gateway. It is recommended to add the endpoints, the gateway, and Integrity Advanced Server to the trusted zone.
- Apply the policy to your new IP catalog.

For information about these tasks, see the *Integrity Advanced Server Administrator Guide*.

Chapter 7

Configuring the Cisco Aironet 1100 Series Wireless Access Point

This chapter contains vendor-specific directions for configuring your Cisco Aironet 1100 Series Wireless Access Point (WAP) to enable Cooperative Enforcement with Integrity Server. Before performing the procedures in this chapter, make sure you have read , Network Access Server Integration and have already completed the procedures covered there. The information provided here assumes that you have already installed and configured the Integrity Server and an Internet Authentication Service.

This chapter covers the following topics:

System Requirements

These are the general components you will need to integrate your Cisco Aironet gateway with Integrity Advanced Server. For more specific system requirements and version information, see the Integrity Advanced Server System Requirements document.

Server Requirements

- Cisco Aironet 1100 Series Wireless Access Point configured for 802.1x and RADIUS authentication
- Firmware 1.09 or later

Client Requirements

- Integrity client 6.0 or later
- One of the following operating systems:

Operating System	EAP Extension Required?
Windows XP	No
Windows 2000	Yes

EAP extensions are available from Microsoft.

Configuring Cisco Aironet 1100 Series Wireless Access Point

This section lists the tasks you must perform to configure Cooperative Enforcement for the Cisco Aironet 1100 Series Wireless Access Point.

To configure the gateway:

1 Perform the network access server integration, as described in "Network Access Server Integration."

2 Create a Cooperative Enforcement SSID. ***See page 102.***

3 Define a Wired Equivalent Privacy Key. ***See page 103.***

4 Define Integrity as the RADIUS server. ***See page 103.***

5 Set the reauthentication interval. ***See page 104.***

Creating a Cooperative Enforcement SSID

Users connect from an endpoint computer to the access point using a Service Set Identifier (SSID). This section explains how to create a new Cooperative Enforcement SSID.

If you already have an SSID that you want to configure for Cooperative Enforcement, edit the SSID with the settings in step **4**. You do not need to change any other information in your configuration.

To create a Cooperative Enforcement SSID:

1 In the Cisco Aironet 1100 Series Management Interface, select **Security** | **SSID Manager**.

2 In the **Current SSID List**, select **<NEW>**.

The fields appear blank.

3 In the **SSID** field, enter a *name* for the SSID.

The SSID is the connection name used by the endpoint computer.

4 Complete the form with the following information:

a If your access point is set up with a VLAN, select the VLAN number from the **Default VLAN** drop-down list. Otherwise, leave this field blank.

If there is a VLAN, you must enter the VLAN ID (number) and Filter ID when creating the gateway catalog on Integrity Server.

b Under Authentication Methods Accepted, select **Open Authentication** and **Add**. In the **Add** drop-down list, choose **EAP**.

c Under Authentication Methods Accepted, select **Network EAP**.

5 Click **Apply**.

The new SSID for Cooperative Enforcement appears in the Current SSID List.

Defining a Wired Equivalent Privacy (WEP) Key

Define a WEP key to encrypt wireless transmissions.

To define a WEP key:

1 In the Cisco Aironet 1100 Series Management Interface, select **Security** | **Encryption Manager.**

2 Define the WEP key as appropriate for your installation.

Be sure to change your WEP keys frequently to enhance the security of your wireless transmissions.

Defining Integrity as the RADIUS Server on the NAS

On the NAS, define Integrity as the RADIUS server.

If you track accounting on the RADIUS server, define a second server with the Internet Authentication Service information and select Use Server For: Accounting. This will send the accounting data directly to the Internet Authentication Service.

To define Integrity as the RADIUS server:

1 In the Cisco Aironet 1100 Series Management Interface, select **Security** | **Server Manager**.

2 From the **Current Server List**, select **New**.

The fields appear blank.

3 Fill in the following information:

a From the **Server Type** drop-down list, select **RADIUS**.

b In the **Server** field, enter the Integrity Advanced Server *hostname* or *IP address*.

c Type the secret in the **Shared Secret** field. The secret must be the same value you used for the "NAS Secret" when creating the gateway catalog on Integrity Advanced Server.

d In **Use Server For**, select *only* **EAP Authentication**.

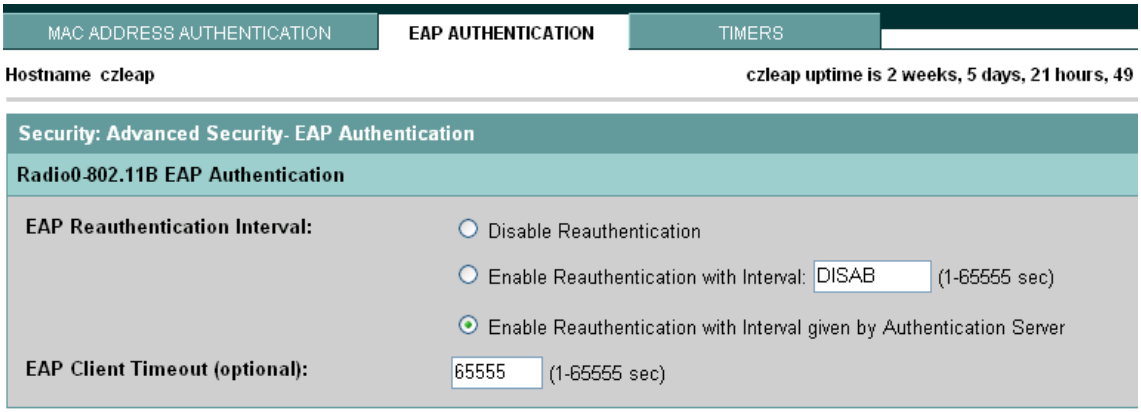
4 Click **Apply** to save the definition.

Setting the Reauthentication Interval

Configure the gateway to use the reauthentication interval defined on the RADIUS server.

To set the reauthentication interval:

1. In the Cisco Aironet 1100 Series Management Interface, select **Security** | **Advanced Security**.
2. Click the **EAP Authentication** tab.
3. Select **Enable Reauthentication with Interval given by Authentication Server**.



Configuring Endpoint Computers

After configuring the NAS, configure the endpoint computer so it can use the wireless access point. For details, see “Configuring Endpoints for Use with Wireless Access Points,” on page 25.

Troubleshooting

This section gives troubleshooting information specific to the Cisco Aironet 1100 Series Wireless Access Point. For general troubleshooting tips, see the "Network Access Server Integration""Network Access Server Integration" chapter.

Symptom: Non-Compliant Users Cannot Establish a Connection

If Reject the Connection is enabled for the gateway catalog on Integrity Advanced Server, users must be compliant to access the network. (For information on the Reject the Connection option, see the instructions on gateway catalogs in the *Integrity Advanced Server Administrator Guide* and the associated online help.)

When Reject the Connection is enabled, Integrity only rejects clients if they do not comply with the assigned policy. If you change the policy assignment when the user is not connected, the client gets the new policy the next time he or she attempts to connect.

Workaround

Non-compliant users must connect to the internal network via a Local Area Network connection and receive the current policy. Users can then establish a wireless connection. (Make sure Integrity is configured to assign endpoints the same policy whether they access the network by wireless or wired LAN connection.)

Chapter 8

Configuring the Cisco Catalyst 2950

This chapter contains vendor-specific directions for configuring your Cisco Catalyst 2950 G Switch to enable Cooperative Enforcement with Integrity Advanced Server. Before performing the procedures in this chapter, make sure you have read , Network Access Server Integration and have already completed the procedures covered there. The information provided here assumes that you have already installed and configured Integrity and an Internet Authentication Service.

This document contains the following sections:

Requirements

These are the general components you will need to integrate your Cisco Catalyst switch with Integrity Advanced Server. For more specific system requirements and version information, see the Integrity Advanced Server System Requirements document.

Server Requirements

- Cisco Catalyst 2950 G Switch configured for RADIUS authentication

Client Requirements

- Integrity client 6.0 or later
- One of the following operating systems:

Operating System	EAP Extension Required?
Windows XP	No
Windows 2000	Yes

EAP extensions are available from Microsoft.

Configuring Cisco Catalyst 2950 G Switch

This section explains how to configure Integrity on the Cisco Catalyst 2950 G Switch.

To configure the Integrity Gateway:

1. Perform the network access server integration, as described in , “Network Access Server Integration.”
2. Use the command prompt to configure Integrity. Use this example as a model:

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
ip subnet-zero
!
vtp domain bob
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
vlan 117
 name Guest
!
vlan 120
!
```

```
interface FastEthernet0/15
 switchport mode access
 dot1x port-control auto
 dot1x timeout reauth-period 300
 dot1x timeout supp-timeout 60
 dot1x timeout server-timeout 160
 dot1x reauthentication
 spanning-tree portfast
!
interface Vlan117
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan120
 ip address 172.16.20.252 255.255.255.0
 no ip route-cache
ip default-gateway 172.16.20.1
ip http server
!
access-list 101 permit ip any host 172.16.211.161
radius-server host 172.16.20.227 auth-port 1814 acct-port 1815
radius-server retransmit 3
radius-server key password
!
end
```

Configuring the Endpoint Computers

After you configure the switch, configure the endpoint computer. For details, see “Configuring Endpoints for Use with Wired Connections,” on page 30.

Troubleshooting

This section gives troubleshooting information specific to the Cisco Catalyst 2950 G Switch. For general troubleshooting tips, see , “Network Access Server Integration.”

Symptom: After Logging Off, the User is Restricted to the VLAN

After logging off (as opposed to shutting down the computer), the user cannot be reauthenticated. Integrity therefore places the user on the restricted VLAN, even if the endpoint computer is compliant. Integrity does not currently support host-based authentication for EAP connections.

Workaround

Reboot the endpoint machine to reauthenticate.

Chapter 9

Configuring the Enterasys RoamAbout R2

This chapter contains vendor-specific directions for configuring your Enterasys RoamAbout R2 wireless access platform to enable Cooperative Enforcement with Integrity Server. Before performing the procedures in this chapter, make sure you have read , Network Access Server Integration and have already completed the procedures covered there. The information provided here assumes that you have already installed and configured the Integrity Server and an Internet Authentication Service.

This chapter covers the following topics:

System Requirements

These are the general components you will need to integrate your Enterasys RoamAbout with Integrity Advanced Server. For more specific system requirements and version information, see the Integrity Advanced Server System Requirements document.

Server Requirements

- Enterasys RoamAbout R2 configured for 802.1x and RADIUS authentication

Client Requirements

- Integrity client 6.0 or later
- One of the following operating systems:

Operating System	EAP Extension Required?
Windows XP	No
Windows 2000	Yes

EAP extensions are available from Microsoft.

Configuring Enterasys RoamAbout R2

This section lists the tasks you must perform to configure Cooperative Enforcement for the Enterasys RoamAbout R2.

Perform the following tasks to configure the gateway:

1 Perform the network access server integration, as described in , “Network Access Server Integration.”

2 Define a Wired Equivalent Privacy Key. ***See page 115.***

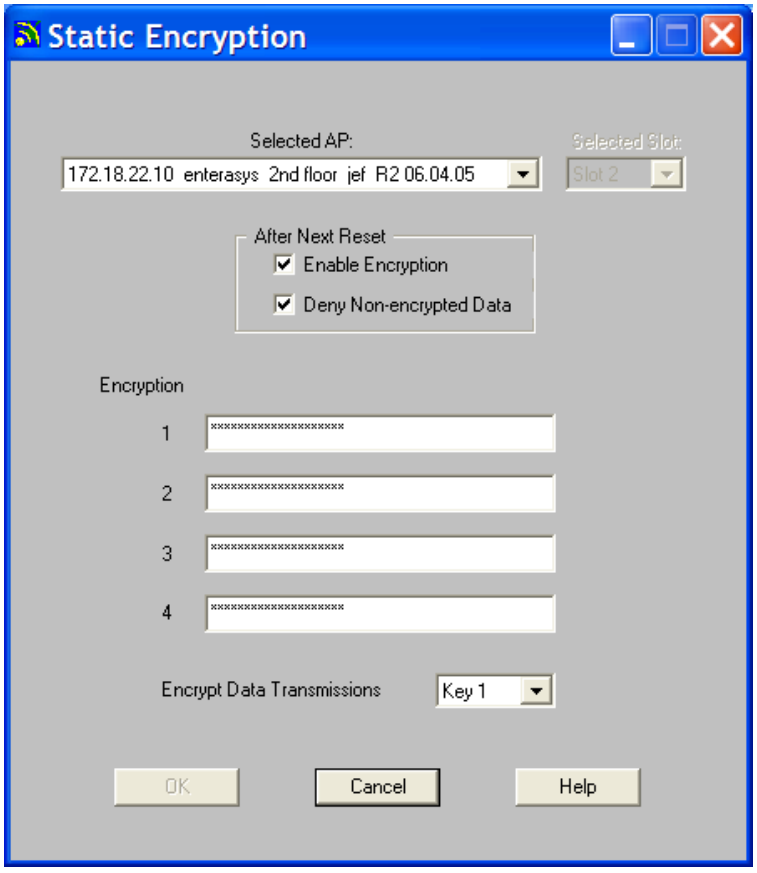
3 Define Integrity as the RADIUS proxy server. ***See page 116.***

Defining a Wired Equivalent Privacy (WEP) Key

Define a WEP key to encrypt wireless transmissions.

To define a WEP key:

1 Open the RoamAbout Access Platform Manager, select the appropriate RoamAbout access platform, and click **Static Encryption**.



2 Define the WEP key as appropriate for your installation.

3 Click **OK**.

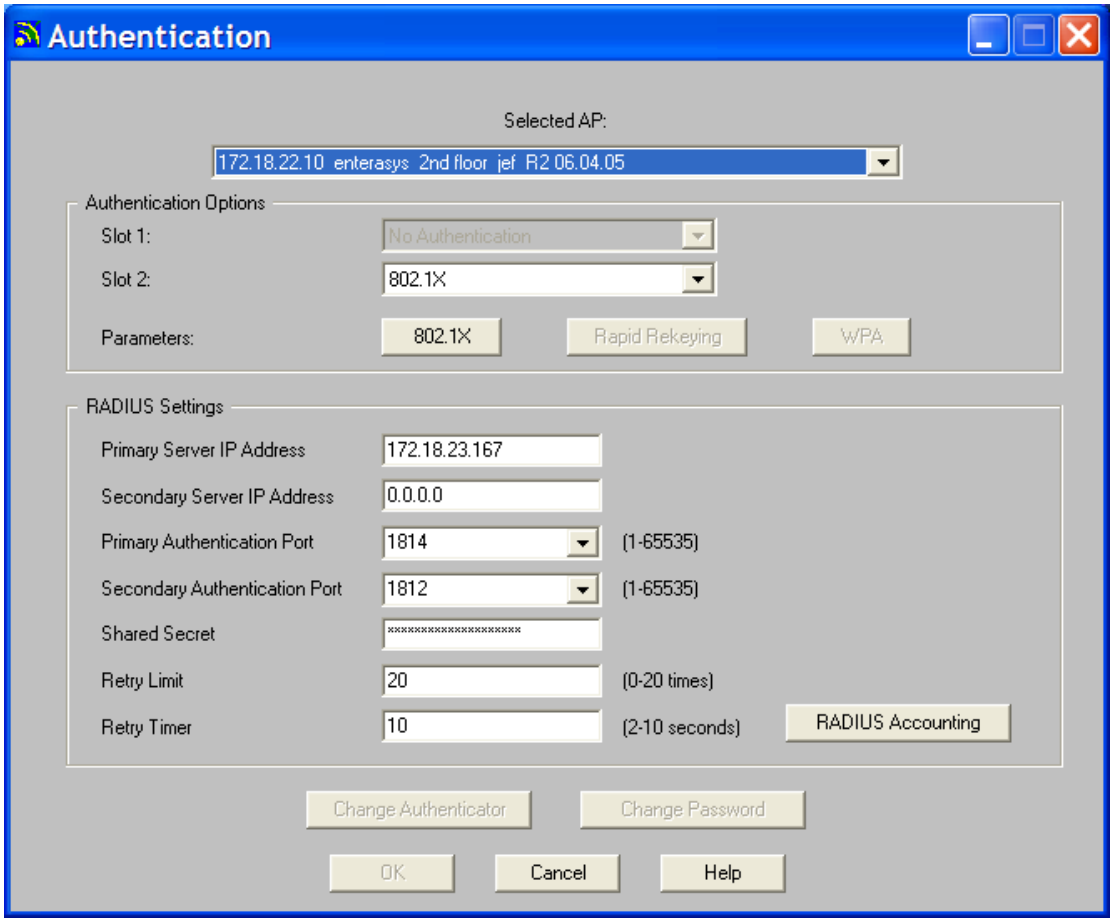
Be sure to change your WEP keys frequently to enhance the security of your wireless transmissions.

Defining Integrity as the RADIUS Server on the NAS

On the NAS, define Integrity as the RADIUS server.

To define Integrity as the RADIUS server:

1 Open the RoamAbout Access Platform Manager, select the relevant RoamAbout access platform, and click **Authentication**.



2 In the Authentication dialog box, do the following:

a In the relevant **Slot** dropdown list, select **802.1x**.

b In the **Primary Server IP Address** field, type the Integrity Advanced Server IP address or hostname.

c In the **Primary Authentication Port** field, type the authentication port number.

d In the **Shared Secret** field, type the secret. The secret must be the same value you used for the "NAS Secret" when creating the gateway catalog on Integrity Advanced Server.

3 Click **OK**.

Configuring Endpoint Computers

After configuring the NAS, configure the endpoint computer so it can use the wireless access point. For details, see “Configuring Endpoints for Use with Wireless Access Points,” on page 25.

Chapter 10

Configuring the Check Point Safe@Office 425W

This chapter contains vendor-specific directions for configuring your Check Point Safe@Office 425W wireless access point (WAP) to enable Cooperative Enforcement with Integrity Server. Before performing the procedures in this chapter, make sure you have read , Network Access Server Integration and have already completed the procedures covered there. The information provided here assumes that you have already installed and configured Integrity Advanced Server and an Internet Authentication Service.

This chapter covers the following topics:

System Requirements

These are the general components you will need to integrate your Check Point Safe@Officee gateway with Integrity Advanced Server. For more specific system requirements and version information, see the Integrity Advanced Server System Requirements document.

Server Requirements

- Check Point Safe@Office 425W configured for 802.1x and RADIUS authentication

Client Requirements

- Integrity client 6.0 or later
- One of the following operating systems:

Operating System	EAP Extension Required?
Windows XP	No
Windows 2000	Yes

EAP extensions are available from Microsoft.

Configuring the Safe@Office 425W

This section lists the tasks you must perform to configure Cooperative Enforcement for the Check Point Safe@Office 425W.

Perform the following tasks to configure the gateway:

1. Perform the network access server integration, as described in , “Network Access Server Integration.”
2. Configuring the wireless settings. ***See page 121.***
3. Define Integrity as the RADIUS proxy server. ***See page 122.***

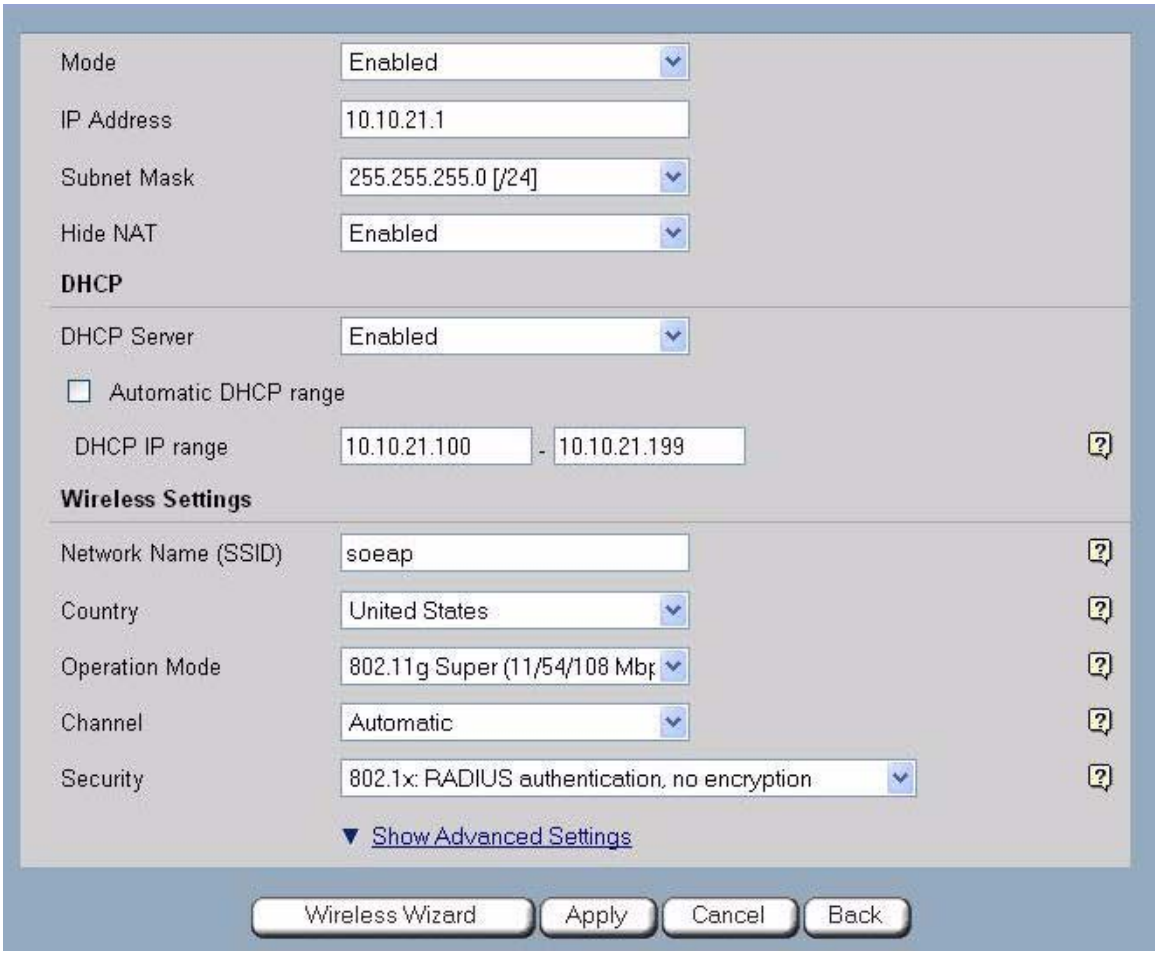
Configuring the Wireless Settings

This section explains how to configure wireless settings.

To configure wireless settings:

1. In the Safe@Office administration console, select **Network** and click the **My Network** tab.

2 In the appropriate WLAN entry, click **Edit**.



3 Type the SSID in the **Network Name (SSID)** field.

4 From the **Security** dropdown list, choose **802.1x RADIUS authentication, no encryption**.

5 Fill out the other fields as appropriate for your installation.

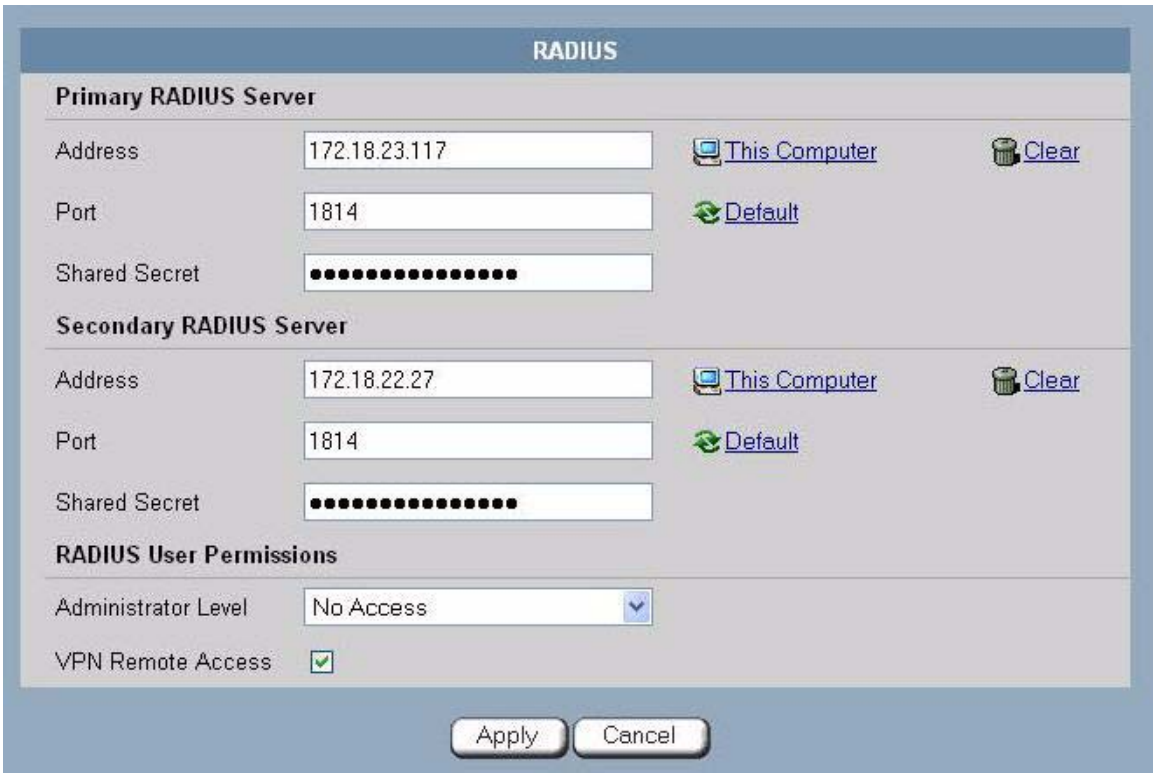
6 Click **Apply**.

Defining Integrity as the RADIUS Server on the NAS

On the NAS, define Integrity as the RADIUS server.

To define Integrity as the RADIUS server:

1 In the Safe@Office administration console, select **Users** and click the **RADIUS** tab.



2 In the Primary RADIUS Server area:

   a Type the Integrity Advanced Server IP address in the **Address** field.

   b Type the port number in the **Port** field.

   c Type the secret in the **Shared Secret** field. The secret must be the same value you used for the "NAS Secret" when creating the gateway catalog on Integrity Advanced Server.

3 Fill out the other fields as appropriate for your installation.

4 Click **Apply**.

Configuring Endpoint Computers

After configuring the NAS, configure the endpoint computer so it can use the wireless access point. For details, see “Configuring Endpoints for Use with Wireless Access Points,” on page 25.

Index