Integrity Advanced Server

Installation Guide

Version NGX 6.6

1-0276-0660-2006-02-24

Contents

Preface

This preface provides an overview of Integrity Advanced Server documentation.

It contains the following topics:

- "About this Guide," on page 9
- "Other Documentation," on page 10

About this Guide

The Integrity Advanced Server Installation Guide provides detailed instructions for installing, configuring, and maintaining Integrity Advanced Server. This document is intended for global administrators. 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 to install Integrity Advanced Server, you should read and understand the information in the Integrity Advanced Server Implementation Guide in order to familiarize yourself with the basic features and principles.

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," on page 10
- "Client Documentation for Administrators," on page 10
- "Client Documentation for Endpoint Users," on page 11
- "Other Documentation," on page 11

Server Documentation for Administrators

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

Table 2-1: Server Documentation for Administrators

Title	Description
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 Administrator Guide	Contains 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.

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 2-2: 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.

Table 2-2: Client Documentation for Administrators

Title	Description
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 2-3: 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.

Other Documentation

The following documentation is intended for Administrators.

Table 2-4: Other documentation

Title	Description
Integrity Advanced Server System Requirements	Contains information on client and server requirements and supported third party devices and applications.

Table 2-4: Other documentation

Title	Description
Integrity Advanced Server Gateway Integration Guide	Contains information on integrating your gateway device with Integrity Advanced Server. It also contains information regarding deploying the unified SecureClient/Integrity client package.

Chapter 1

Integrity Advanced Server Overview

This chapter describes Integrity Advanced Server components and communications.

- "Integrity Advanced Server system components," on page 14
- "Integrity Advanced Server communications," on page 17

Integrity Advanced Server system components

This section provides an overview of the Integrity Advanced Server system components.

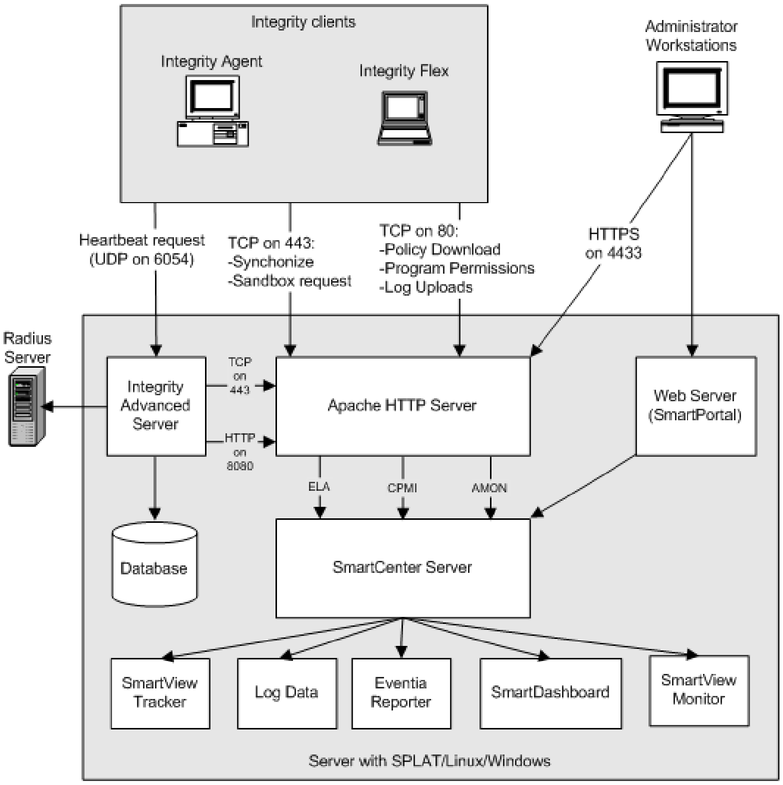
System requirements

For information about Integrity Advanced Server system requirements, see the Integrity Advanced Server System Requirements Document on the Check Point Web site.

Architecture

Figure 3-1 shows a typical installation. In this illustration, the Integrity Advanced Server system components are mostly installed on a single host. There are several other configurations options available, some involving distributing one or more components across multiple servers. Figure 3-1 illustrates the relationships and communications between the components, which is the same for all installations. For more information about the other configurations, see "Installing and Configuring the Integrity Advanced Server," on page 21.

Figure 3-1: typical Integrity Advanced Server Configuration



A typical Integrity Advanced Server configuration includes the following components:

- **Integrity Advanced Server**-Allows you to centrally configure your Integrity enterprise policies.

- **Integrity Clients**-Monitor your endpoints and enforce your security policies. These clients are installed on your endpoint computers. There are two types of Integrity clients that work with Integrity Advanced Server:
  - **Integrity Flex-**has a full user interface that allows the user to control security settings under some conditions.
  - **Integrity Agent**- Has a limited interface and does not allow the user to control his or her security settings.
- **Database**-Integrity includes an embedded database, but you may also use a third-party database with the system. For information about supported databases, see the Integrity Advanced Server System Requirements document on the Check Point Web site. For more information about how to configure your databases, see "Configuring the databases and gathering information," on page 22.
- **Apache HTTP Server**-Provides secure HTTPS communication between the Integrity Advanced Server and Integrity clients. It also provides secure communication with the Integrity Advanced Server for Administrators logging onto the Integrity Advanced Server Administrator Console. The Apache HTTP server also improves performance by serving your security data to Integrity clients.
- **Administrator Workstation**-Administrators can use a workstation to access Integrity Advanced Server through the Integrity Advanced Server Administrator Console, a Web-based Graphical User Interface that allows Administrators to create security policies, view reports, and perform other administrative tasks.
- **RADIUS Server**-You can optionally connect your RADIUS server to the Integrity Advanced Server system to provide authentication. Integrity Advanced Server comes with built-in administrator authentication. For more information, see "Configuring the RADIUS Server," on page 63.
- **Other Check Point Components**-When you install Integrity Advanced Server, you are also automatically installing some Check Point SmartCenter components to create an integrated security solution. These components are installed in the background even if you choose an 'Integrity only' installation. Integration points include:
  - Smart Portal-
  - SmartCenter Server
  - SmartView Tracker
  - Eventia Reporter
  - SmartDashboard
  - SmartView Monitor
  - Logging

  For more information about these integration points, see "Integrations With Other Check Point products," on page 13.

Integrity Advanced Server also integrates with a variety of gateways, such as VPN or wireless devices, to provide client enforcement capabilities at the gateway level. for more information about these sorts of configurations, see “Gateways and Cooperative Enforcement,” on page 172 of the Integrity Advanced Server Administrator Guide and the chapter of the Integrity Advanced Server Gateway Integration Guide appropriate to your gateway device. The Integrity Advanced Server System Requirements document lists all supported gateways. These documents are available on the Check Point Web site.

Integrity Advanced Server communications

This section explains the internal and external communication protocols and ports used by the Integrity system.

When an Integrity client is initialized it performs a sync with the Integrity Advanced Server. This allows the Integrity client to get the security policy that is assigned to it. Other communications take place either by the request of administrators or as determined by your security policies.

The Integrity Advanced Server Sync

1. The Integrity client requests the policy location from the Integrity Advanced Server.
2. The server returns a sync response to the Integrity client with the location of the policy.
3. The client then downloads the policy assigned to it. This is done over TCP on port 80. The Web server transmits the request to the Integrity Advanced Server over HTTP on port 8080. The policy contains both your security policy information as well as the location of the remediation sandbox and log upload server.

   Once the Integrity client receives the policy, it immediately enforces it.

Other Integrity Advanced Server Communications

Once the sync has been established between the Integrity Advanced Server and the Integrity client, the following types of communication may occur, depending on circumstances and the security policy you configure.

- **Heartbeats-**Once the sync request has completed successfully, a heartbeat will regularly occur based on the interval specified in the security policy. Heartbeats occur over UDP on port 6054. Heartbeats contain various pieces of information concerning the status and compliance state of the endpoint computer. This information is stored in the Integrity database and is used for the Integrity Monitor report.
- **Remediation Requests-**The Integrity client may request remediation resources from the Integrity Advanced Server sandbox.

  For example, if the client is out of compliance with the policy's enforcement rules, the policy might specify that the client should restrict the endpoint computer's access to your network and attempt to download a remediation file from the sandbox remediation area. The initial Integrity client connection to the sandbox is done over TCP on port 443, while the download is done on port 80 because the Integrity client verifies the sandbox files after download by checking the MD5 hash.
- **Program Permission Requests**-Depending on your policy settings, as programs are run on the endpoint computer, Integrity clients may request program permission information from the Integrity Advanced Server. These real-time requests are performed over TCP on port 80.

- **Log Upload**-Periodically, the Integrity client uploads logs to the Integrity Advanced Server. These logs are stored in SmartCenter's log data files using the ELA API. You can configure the frequency of the log upload using the Integrity Advanced Server Administrator console.
- **Administrator Workstation Access-**Administrators can use a workstation to access the Integrity Advanced Server Administrator console to make changes to configure security policies, view reports and perform other administration tasks. The administrator workstation contacts the Integrity Advanced Server via HTTPS on port 443. Some reports are viewed on SmartPortal via HTTPS on port 4433 by drilling down in the Integrity Advanced Server Administrator console.

Integrity Advanced Server Services

Integrity Advanced Server operations are implemented by separate Integrity services.

The services are divided into two types:

- **Client services** allow an Integrity client to get policies and configuration information, and to communicate session state information.
- **Administration services** allow administrators to create groups and users; manage policies; manage system configuration; and perform other administrative tasks.

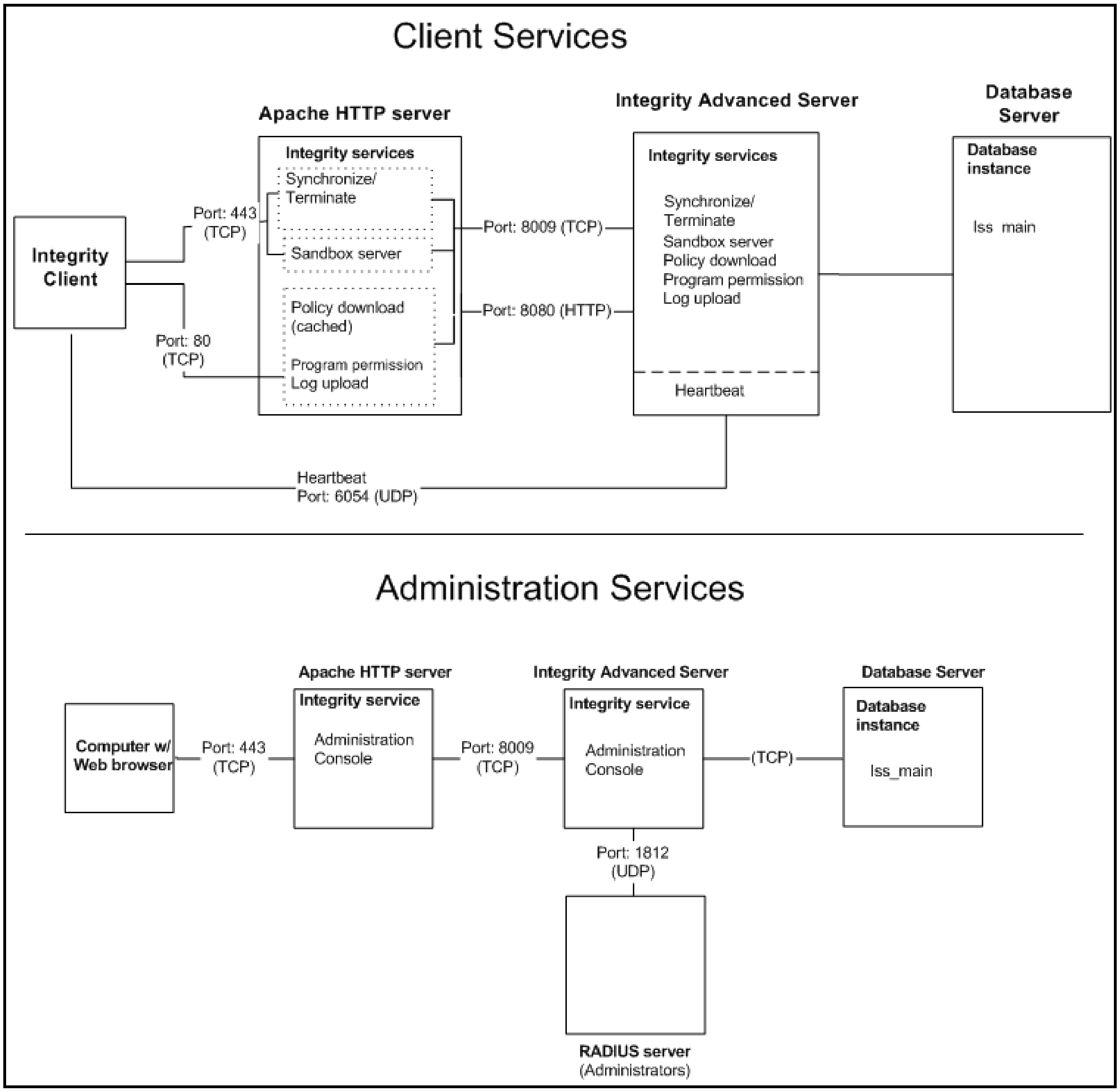
Services and Ports

Integrity Advanced Server uses the ports listed below to communicate with Integrity clients. Make sure all these ports are available on the Integrity Advanced Server:

- 80
- 443
- 6054
- 8009
- 8010

"Integrity Advanced Server services and ports," on page 19 represents the services that make up Integrity Advanced Server and shows which ports the services use.

Figure 3-2: Integrity Advanced Server services and ports



Service Details

The table below lists the individual services that make up the Integrity Advanced Server. The configuration name is the parameter name of the service in the Integrity Advanced Server and Apache HTTPS server configuration files. The URL is the service location information embedded in the request from the Integrity client that allows the Apache HTTPS server to proxy requests.

Table 3-1: Description of Integrity Services

Service name	Configuration Name	URL	Description
Connection Manager	service.enable.connectionManager	/cm/*	Sychronizes with the server. The Connection Manager service allows the endpoint to establish a session, verify endpoint state information, and get information needed to download the current policy and configuration. It can also end a previously synchronized session with the endpoint. this service also sends heartbeats to communicate policy or state changes
Policy download	service.enable.policy	/policy/*	Policy download service.
Log upload	service.enable.logUpload	/logupload/*	Provides the mechanism endpoint computers use to upload client log files.
Program permission	service.enable.logUpload	/ask/*	Provides the mechanism endpoint computers use to upload client log files.
Sandbox server	service.enable.sandBox	/sandbox/*	Serves remediation Web pages to non-compliant, authenticated endpoint users.
Package Manager	service.enable.package	/package/*	Serves the client installer packages that install an Integrity client on an endpoint computer.
Administrator Console	service.enable.adminConsole	/	Serves the user interface that allows administrators to manage the Integrity Advanced Server.

Chapter 2

Installing and Configuring the Integrity Advanced Server

This chapter describes the configuration and installation steps you need to perform to get your Integrity Advanced Server system up and running. It covers the following topics:

Overview of installation options

You can install Integrity Advanced Server as a standalone product or with other Check Point products, such as SmartCenter or VPN-1. If you choose to install Integrity Advanced Server with other Check Point products, you can install it on the same server, or on a dedicated host.

For all installation options, you use a master installer that lets you select which products to install. Note that all IAS installations (standalone or integrated) include Check Point SmartPortal, which provides some of IAS's reporting functionality. If you choose standalone mode, the installer also silently installs some necessary components of Check Point SmartCenter, which remain invisible.

See the following sections for more informaiton about your installation options:

- "Installing Integrity on a dedicated host," on page 25.
- "Installing Integrity Advanced Server with other Check Point products," on page 31

Before you begin

Before you install Integrity Advanced Server, configure the database you plan to use with IAS and synchronize the database clock with the IAS host clock. This section covers the following topics:

- "Configuring the databases and gathering information," on page 22
- "Synchronizing Clocks," on page 25

Configuring the databases and gathering information

The Integrity Advanced Server stores operational and logging information in a database. You can use any of the following databases with Integrity Advanced Server:

Database	Version	JDBC version
Oracle	9.2.0.4.0	ojdbc14.zip (download from Oracle)
SQL Server	2000 SP3a	SQL Server Driver for JDBC SP3 (download from Microsoft)
JDataStore (Embedded)	7.2	Bundled with JDataStore

If you use the embedded database, it will be automatically configured by the Integrity Advanced Server Installer and you can skip the steps in this section.

Before you configure Integrity Advanced Server, configure your database and gather the necessary information.

To ensure good performance, you may have to periodically perform database maintenance. For more information about maintaining your database, see Chapter 8, “Maintaining Integrity Advanced Server,” on page 88.

To configure Oracle 9*i*:

1. Create your database.

   Be sure to specify the UTF-8 character set. Due to the length of some of the indexes, the minimum recommended block size for an Oracle database is 4096.

2. Record the database server host name.

> Use a host name rather than an IP address to specify your database. This allows you to later change your database.

3. Record your database port for connections with the Integrity Advanced Server. The default port number for communications with Oracle 9*i* is 1521.
4. Create a user with the name ‘iss_main’ with a matching schema name.
5. Assign the user the ‘CONNECT’ and ‘RESOURCE’ roles and grant the following system privileges:
   - QUERY REWRITE
   - ALTER ANY PROCEDURE
   - CREATE ANY PROCEDURE
   - DROP ANY PROCEDURE
   - EXECUTE ANY PROCEDURE
   - UNLIMITED TABLESPACE
6. In the Enterprise Manager Console, in Network | Databases | <database name> | Instance | Configuration set the following parameters:
   - QUERY_REWRITE_INTEGRITY = TRUSTED
   - QUERY_REWRITE_ENABLED = TRUE
   - NLS_SORT= <blank>
7. Record the database username and password for the Integrity Advanced Server.

To configure SQL Server:

1. Create your database.

2. Record your database server host name.

> Use a host name rather than an IP address to specify your database. This allows you to later change your database.

3. Record your database port for connections with the Integrity Advanced Server. The default port number for communications with SQL Server is 1433.

4. Create a database login.

   The database login must have the following roles:

   - public
   - db_owner
   - ddl_admin
   - db_datareader
   - db_datawriter

> The database login must not have the system administrator role.

5. Create the Integrity Advanced Server database.

   The preconfigured database name in Integrity Advanced Server is iss_main.

6. Use the Enterprise Manager (found in the properties for the server instance) to set your authentication types.

   In order for the JDBC drivers to log in correctly, your SQL Server security must be set up to handle both SQL authentication and Windows authentication (Mixed Mode). The JDBC drivers use a SQL authenticated user and password and will not be able to connect if SQL Server is configured for Windows security authentication only.

7. Set the recovery model to simple.

   By default, SQL Server Enterprise uses “FULL” recovery mode. This means that all transactions are logged until the database is backed up. This requires a log file that is at least as large as the database file. As an alternative it is recommended that you set the SQL Server recovery mode to **Simple**. Setting the recovery mode to simple truncates the log at certain intervals. Be aware that if you choose to set the recovery mode to simple and a server crashes, the data can only be recovered to the last full or differential backup.

> Perform this tuning operation during intervals that do not effect the performance of your Integrity environment.

   a. Open the SQL Server Enterprise Manager.

   b. Highlight the Integrity database.

c. Right-click on the entry and select **Properties**.

d. Click the **Options** tab.

e. For **Model**, select **Simple**.

f. Click **OK**.

Alternatively, you can also set the recovery mode to simple using the following command:

```
exec sp_dboption N'integrity', N'trunc. log', N'true'
```

8. Record the database username and password for Integrity Advanced Server.

Synchronizing Clocks

It is recommended that you synchronize the clocks on the Integrity Advanced Server host with those on your database. In a distributed installation (in which Integrity Advanced Server and SmartCenter are installed on separate hosts), you must synchronize clocks as well ensure that both hosts are in the same time zone.

To synchronize clocks in Linux:

1. Use the ntpdate command to synchronize with public network time protocol (NTP) servers every 15 minutes.

```
$ ntpdate <primary NTP server> <secondary NTP server>
```

To synchronize clocks in Windows:

1. Use a third party synchronization tool to synchronize with NTP servers every 15 minutes.

Installing Integrity on a dedicated host

This section explains how to install Integrity Advanced Server on a dedicated server. The instructions apply to Integrity standalone installations (with no SmartCenter integration) as well as to the Integrity portion of distributed installations (in which Integrity and either SmartCenter or Provider-1 are installed on separate hosts). Follow the instructions appropriate for your operating system. Where necessary, the instructions refer you to more detailed explanations in subsequent sections.

The IAS installer is contained in a master installer that includes options for installing other Check Point products with which you can integrate Integrity Advanced Server. When installing Integrity Advanced Server without any other Check Point products, ignore the options for installing other products. Note, however, that IAS installations always include Check Point SmartPortal, which provides some of IAS's reporting functionality. The installer also silently installs some necessary Check Point SmartCenter components.

If you are installing Integrity in standalone mode, the log server is installed on the same host as Integrity. If you prefer to install the log server on a remote host, see "Remote logging," on page 55.

To learn how to install Integrity Advanced Server with other Check Point products (such as SmartCenter or VPN-1), skip this section and see "Installing Integrity Advanced Server with other Check Point products," on page 31.

Windows

To install IAS on Windows:

1. On the intended host server, double-click the setup.exe file.

   The Check Point master installer begins.

2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. Choose **Check Point Enterprise / Pro** and click **Next**.
5. Choose **New Installation** and click **Next**.
6. Choose **Integrity**, making sure to deselect any other default selections. Click **Next**.
7. Do one of the following:
   - If you are installing Integrity in standalone mode, choose **Integrity Standalone** and click **Next**.
   - If you are installing Integrity as part of a distributed installation (in which SmartCenter or Provider-1 runs on another host), choose **Integrity with Remote SmartCenter** and click **Next**.
8. Click **Next** to start the installation.

   An Installation Status bar appears, displaying the chosen installation package. The master installer then starts the IAS installer. (It may take a few minutes to start.)

9. Work through the Integrity Advanced Server installation wizard. For information on completing the wizard, see "The Integrity Advanced Server installer," on page 47.

   When the IAS installer completes, the Check Point Configuration Tool launches.

10. Perform basic configuration steps with the Check Point configuration program. For details, see "The Check Point Configuration Tool," on page 51. (If you are planning to set up a distributed installation with either SmartCenter or Provider-1, be sure to

create and make note of the activation key. You will use this later when establishing communication between Integrity and SmartCenter or Provider-1.)

11. Click **Finish** to close the master installer. Then restart the computer.

Linux

To install IAS on Linux:

1. On the intended host server, go to the installer directory and issue the following command:

   ```
   ./UnixInstallScript
   ```

   The Check Point master installer starts to run.

2. Read the master installer welcome screen and type **N** (for Next).

3. Read the license agreement and type **Y** to accept.

4. Select **Check Point Enterprise / Pro** and press **N**.

   For more information about Check Point Enterprise and Check Point Pro, see the Check Point documentation set.

5. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and press **N**.

6. When the product menu appears, choose **Integrity** by typing the corresponding number. Then type **N** to continue.

7. When prompted to specify the Integrity configuration type, do one of the following:

   - If you are installing Integrity in standalone mode, choose **Integrity Only** (by typing the corresponding number) and type **N**.

   - If you are installing Integrity as part of a distributed installation (in which SmartCenter or Provider-1 runs on another host), choose **Integrity with Remote SmartCenter** (by typing the corresponding number) and type **N**.

8. When the Validation screen appears, verify the installation settings and type **N**.

   The Integrity Advanced Server installation wizard begins.

9. Work through the Integrity Advanced Server installation wizard. For information on completing the wizard, see “The Integrity Advanced Server installer,” on page 47.

   When the Integrity Advanced Server installer completes, the Check Point Configuration Tool launches automatically.

10. Perform basic configuration steps with the Check Point Configuration Tool. For details, see “The Check Point Configuration Tool,” on page 51. (If you are planning to set up a distributed installation with either SmartCenter or Provider-1, be sure to

create and make note of the activation key. You will use this later when establishing communication between Integrity and SmartCenter or Provider-1.)

11. Type **E** to exit the master installer.

Check Point SecurePlatform (Command Line Version)

When installing IAS on SecurePlatform, install the version of SecurePlatform that corresponds to the IAS version you plan to install. The appropriate SecurePlatform version is included on the installation CD.

To install IAS on SecurePlatform:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.

2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see "Installing Check Point SecurePlatform," on page 45.

3. Run the cpconfig command to start the installer.

4. Read the master installer welcome screen and type **N** (for Next).

5. Read the license agreement and type **Y** to accept.

6. Select **Check Point Enterprise / Pro** and type **N**.

7. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and type **N**.

8. When prompted to specify the Integrity configuration type, do one of the following:

   - If you are installing Integrity in standalone mode, choose **Integrity Only** (by typing the corresponding number) and type **N**.

   - If you are installing Integrity as part of a distributed installation (in which SmartCenter or Provider-1 runs on another host), choose **Integrity with Remote SmartCenter** (by typing the corresponding number) and type **N**.

9. When prompted to specify the Integrity configuration type, choose **Integrity Only** and type **N**.

10. When the Validation screen appears, verify the installation settings and type **N**.

    The Integrity Advanced Server installation wizard begins.

11. Work through the Integrity Advanced Server installation wizard. For information on completing the wizard, see "The Integrity Advanced Server installer," on page 47.

    When the Integrity Advanced Server installer completes, the Check Point Configuration Tool launches automatically.

12. Perform basic configuration steps with the Check Point Configuration Tool. For details, see "The Check Point Configuration Tool," on page 51. (If you are planning

to set up a distributed installation with either SmartCenter or Provider-1, be sure to create and make note of the activation key. You will use this later when establishing communication between Integrity and SmartCenter or Provider-1.)

13. Type **E** to exit the master installer.

14. Press **Enter**, log out by exiting the master installer (by typing **exit** and pressing **Enter**, and then repeating), and then log in again to complete the installation. You can now start the installed product by running **cpstart**.

Check Point SecurePlatform (GUI Version)

When installing IAS on SecurePlatform, install the version of SecurePlatform that corresponds to the IAS version you plan to install. The appropriate SecurePlatform version is included on the installation CD.

To install IAS on SecurePlatform:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.

2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see “Installing Check Point SecurePlatform,” on page 45.

3. Using Internet Explorer, navigate to https://<SPLAT IP>:<Port number>.

   Use the port number you specified during the installation of SecurePlatform. If you are prompted to allow popups, allow them always for this site. The welcome page appears.

4. Click **Next** to continue. In the subsequent pages you will have the opportunity to configure the following:

   - Network Connections
   - Routing Tables
   - DNS Servers
   - Host and Domain Name
   - Device Date and Time
   - Web/SSH Clients

   You may configure any of these you wish, or skip them, depending on your installation needs. Use the **Next** button to proceed through the pages until you reach the **Installation Options** page.

5. Select **Check Point Enterprise / Pro** or **Check Point Express** and click **Next**.

6. Select **Integrity** and **SmartPortal** and click **Next**.

7. Do one of the following:

    - If you are installing Integrity in standalone mode, select **Integrity Only** and click **Next**.

    - If you are installing Integrity as part of a distributed installation (in which SmartCenter or Provider-1 runs on another host), select **Integrity with Remote SmartCenter** and click **Next**.

8. Select **New Installation** and click **Next**.

9. Proceed through the installation wizard, entering the following information for your installation:

    - Integrity Server type

    - Integrity Server information

    - Domain options

    - Clustering options

    - Main database type

    - Client languages

    Use the **Next** button to proceed through the wizard pages. For more information about these options, see "The Integrity Advanced Server installer," on page 47.

10. The Smart Center configuration begins.

    Use the **Next** button to proceed through the configuration pages, entering your information. For more information about these options, see "Configuration tool options," on page 52.

11. Click **Finish** to finish the installation.

12. Confirm the installation. When the installation and configuration process finishes, reboot your computer.

Installing Integrity Advanced Server with other Check Point products

This section explains the high-level steps required to install Integrity Advanced Server with other Check Point products. Follow the instructions appropriate for the desired installation. Where necessary, the instructions refer you to more detailed explanations in subsequent sections.

By default, the log server is installed on the same host as SmartCenter. If you prefer to install the log server on a remote host, see "Remote logging," on page 55.

The following topics are covered:

- "Integrity and SmartCenter on the same host," on page 31
- "Integrity and SmartCenter in a distributed installation," on page 36
- "Integrity and Provider-1," on page 41

Integrity and SmartCenter on the same host

This section describes how to install Integrity Advanced Server and Check Point SmartCenter on a single host. Follow the instructions appropriate for your operating system.

Windows

To install IAS and SmartCenter on Windows:

1. On the intended host server, double-click the setup.exe file.

   The Check Point master installer begins.

2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. Choose **Check Point Enterprise / Pro** and click **Next**.
5. Choose **Demo Installation**, **New Installation**, or **Installation Using Imported Configuration**, as appropriate, and click **Next**. (In this context, the Imported Configuration option does not apply to Integrity Advanced Server. It applies only to other Check Point products.)
6. Choose **SmartCenter** and **Integrity**, making sure to deselect any other default selections. It is recommended to install SmartConsole (Check Point's administration application) on a *separate* host. (For details on installing SmartConsole later on a separate host, see "Installing SmartConsole components,"

on page 45.) If, however, you wish to administer the installation from the current host, select **SmartConsole** as well. Click **Next**.

7. Choose **Primary SmartCenter** and click **Next**.
8. Click **Next** to start the installation.

   The Installation Status bar appears, displaying the chosen installation packages and highlighting the one that is currently active. The master installer automatically launches the installers for the selected products, beginning with the SmartCenter installer.
9. Specify the installation directory or accept the default, and click **Next**.

   The installer begins. It may take a couple minutes.
10. When the SmartCenter installer completes, click **OK**.

    The installer performs configuration in the background for up to five minutes. Do not interrupt the configuration, even if it appears as if nothing is happening. When the configuration is complete, the master installer launches the next package.
11. Do one of the following:
    - If you chose *not* to install SmartConsole on the current host, the master installer launches the IAS installer. Go to step 16.
    - If you chose to install SmartConsole on the current host, the master installer launches the SmartConsole installer. Go to step 12.
12. Specify the installation directory or accept the default, and click **Next**.
13. Select the UI client applications to install or accept the defaults, and click **Next**.
14. When prompted to create desktop shortcuts, click **Yes** or **No**, as desired.
15. When prompted to confirm the successful installation, click **OK** and then click **Finish**.

    The master installer launches the IAS installer. It may take a couple minutes.
16. Work through the Integrity Advanced Server installation wizard. For information on completing the wizard, see "The Integrity Advanced Server installer," on page 47.

    When the IAS installer completes, the master installer launches the SmartPortal installer, which runs silently and requires no administrator input. When the SmartPortal installer completes, the Check Point Configuration Tool launches automatically.

17. Perform basic configuration steps with the Check Point Configuration Tool. For details, see “The Check Point Configuration Tool,” on page 51.

18. Click **Finish** to close the master installer. Then restart the computer.

Linux

To install IAS and SmartCenter on Linux:

1. Log in to the host server with an account that has root privileges.

2. Go to the installer directory and issue the following command:

   ./UnixInstallScript

   The Check Point master installer starts to run.

3. Read the master installer welcome screen and type **N** (for Next).

4. Read the license agreement and type **Y** to accept.

5. Select **Check Point Enterprise / Pro** and type **N**.

6. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and type **N**.

7. When the product menu appears, choose **SmartCenter** and **Integrity** by typing the corresponding numbers. Then type **N** to continue.

   Note that SmartConsole does not run on Linux. To use SmartConsole with a SmartCenter installation on Linux, you must install SmartConsole on another host. (For details on installing SmartConsole, see “Installing SmartConsole components,” on page 45.)

8. Select **Primary SmartCenter** and type **N**.

9. When the Validation screen appears, verify the installation settings and type **N**.

   The SmartCenter installer runs, requiring no user input. When the SmartCenter installer completes, the master installer prompts you to continue.

10. Press **Enter** to continue.

    The Integrity Advanced Server installer begins.

11. Work through the Integrity Advanced Server installation wizard. For information on completing the wizard, see “The Integrity Advanced Server installer,” on page 47.

    When the Integrity Advanced Server installer completes, the Check Point configuration program launches automatically.

12. Perform basic configuration steps with the Check Point configuration program. For details, see "The Check Point Configuration Tool," on page 51.

13. Type **E** to exit the master installer.

Check Point SecurePlatform (Command line Version)

When installing IAS on SecurePlatform, install the version of SecurePlatform that corresponds to the IAS version you plan to install. The appropriate SecurePlatform version is included on the installation CD.

To install IAS and SmartCenter on SecurePlatform:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.

2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see "Installing Check Point SecurePlatform," on page 45.

3. Run the cpconfig command to start the installer.

4. Read the master installer welcome screen and type **N** (for Next).

5. Read the license agreement and type **Y** to accept.

6. Select **Check Point Enterprise / Pro** and type **N**.

7. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and type **N**.

8. When the product menu appears, choose **SmartCenter** and **Integrity** by typing the corresponding numbers. Then type **N** to continue.

   Note that SmartConsole does not run on SecurePlatform. To use SmartConsole with a SmartCenter installation on SecurePlatform, you must install SmartConsole on another host. (For details on installing SmartConsole, see "Installing SmartConsole components," on page 45.)

9. Select **Primary SmartCenter** and type **N**.

10. When the Validation screen appears, verify the installation settings and type **N**.

    The SmartCenter installer runs, requiring no user input. When the SmartCenter installer completes, the Integrity Advanced Server installation wizard begins.

11. Press **Enter** to continue.

12. Work through the Integrity Advanced Server installation wizard. For information on completing the wizard, see "The Integrity Advanced Server installer," on page 47.

    When the Integrity Advanced Server installer completes, the Check Point Configuration Tool launches automatically.

13. Perform basic configuration steps with the Check Point Configuration Tool. For details, see “The Check Point Configuration Tool,” on page 51.
14. Type **E** to exit the master installer.
15. Restart the computer.
16. Press **Enter**, log out by exiting the master installer (type **exit** and press **Enter**, two times), and then log in again to complete the installation. You can now start the installed products by running **cpstart**.

Check Point SecurePlatform (GUI Version)

When installing IAS on SecurePlatform, install the version of SecurePlatform that corresponds to the IAS version you plan to install. The appropriate SecurePlatform version is included on the installation CD.

To install IAS and SmartCenter on SecurePlatform:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.

2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see “Installing Check Point SecurePlatform,” on page 45.
3. Using Internet Explorer, navigate to https://<SPLAT IP>:<Port number>.

   If you are prompted to allow popups, allow them always for this site. The welcome page appears.

4. Click **Next** to continue. In the subsequent pages you will have the opportunity to configure the following:

   - Network Connections
   - Routing Tables
   - DNS Servers
   - Host and Domain Name
   - Device Date and Time
   - Web/SSH Clients

   You may configure any of these you wish, or skip them, depending on your installation needs. Use the **Next** button to proceed through the pages until you reach the **Installation Options** page.

5. Select **Check Point Enterprise / Pro** or **Check Point Express** and click **Next**.
6. Select **SmartCenter, SmartPortal,** and **Integrity**, making sure to deselect any other default selections, and click **Next**.
7. Do one of the following:
8. If you are installing Integrity in standalone mode, select **Integrity Only**and click **Next**.
9. If you are installing Integrity as part of a distributed installation (in which SmartCenter or Provider-1 runs on another host), select **Integrity with Remote SmartCenter** and click **Next**.
10. Select **New Installation** and click **Next**.
11. Proceed through the installation wizard, entering the following information for your installation:

    - Integrity Server type
    - Integrity Server information
    - Domain options
    - Clustering options
    - Main database type
    - Client languages

    Use the **Next** button to proceed through the wizard pages. For more information about these options, see "The Integrity Advanced Server installer," on page 47.
12. The SmartCenter configuration begins.

    Use the **Next** button to proceed through the configuration pages, entering your information. For more information about these options, see "Configuration tool options," on page 52.
13. Click **Finish** to finish the installation.
14. Confirm the installation. When the installation and configuration process finishes, reboot your computer.

Integrity and SmartCenter in a distributed installation

This section describes how to install Integrity Advanced Server and Check Point SmartCenter on separate hosts (a setup known as a distributed installation). Follow the instructions appropriate for your operating system. Note that, when setting up a distributed installation, you can install Integrity and SmartCenter on different operating systems. For example, Integrity can run on Windows while SmartCenter runs on Linux.

By default, the log server is installed on the same host as SmartCenter. If you prefer to install a remote log server, perform step 3 in the procedure below.

To install Integrity and SmartCenter on separate hosts:

1. Install Integrity Advanced Server on one host. (See "Installing Integrity on a dedicated host," on page 25.)
2. Install SmartCenter on another host. (See "Installing SmartCenter in a distributed installation," on page 37.)

> The Integrity Advanced Server host and the SmartCenter host must be set to the same time zone.

3. Install a log server on a third (remote) host. (See "Installing the log server remotely," on page 55.)
4. Configure the communication between Integrity, SmartCenter, and the remote log server. (See "Connecting Integrity and SmartCenter," on page 53; and, if applicable, "Configuring remote logging," on page 59.)

Installing SmartCenter in a distributed installation

Follow the directions appropriate for your operating system.

Windows

To install SmartCenter in a distributed installation:

1. On the intended host server, double-click the setup.exe file.

   The Check Point master installer begins.
2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. Choose **Check Point Enterprise / Pro** and click **Next**.
5. Choose **Demo Installation**, **New Installation**, or **Installation Using Imported Configuration**, as appropriate, and click **Next**.
6. Choose **SmartCenter**, making sure to deselect any other default selections. It is recommended to install SmartConsole (Check Point's web administration application) on a *separate* host. (For details on installing SmartConsole later on a separate host, see "Installing SmartConsole components," on page 45.) If, however, you wish to administer the installation from the current host, select **SmartConsole** as well. Click **Next**.
7. Choose **Primary SmartCenter** and click **Next**.
8. Click **Next** to start the installation.

   The Installation Status bar appears, displaying the chosen installation package(s). The master installer automatically launches the SmartCenter installer.

9. Specify the installation directory or accept the default, and click **Next**.

   The installer begins. It may take a couple minutes.

10. When the SmartCenter installer completes, click **OK**.

    The installer performs configuration in the background for up to five minutes. Do not interrupt the configuration, even if it appears as if nothing is happening.

11. Do one of the following:

    - If you chose *not* to install SmartConsole on the current host, the Check Point Configuration Tool launches automatically. Go to step 16.

    - If you chose to install SmartConsole on the current host, the master installer launches the SmartConsole installer. Go to step 12.

12. Specify the installation directory or accept the default, and click **Next**.

13. Select the UI client applications to install or accept the defaults, and click **Next**.

14. When prompted to create desktop shortcuts, click **Yes** or **No**, as desired.

15. When prompted to confirm the successful installation, click **OK** and then click **Finish**.

    When the SmartConsole installer completes, the Check Point Configuration Tool launches automatically.

16. Perform basic configuration steps with the Check Point Configuration Tool. For details, see "The Check Point Configuration Tool," on page 51.

17. Click **Finish** to close the master installer. Then restart the computer.

Linux

To install SmartCenter in a distributed installation:

1. Log in to the host server with an account that has root privileges.

2. Go to the installer directory and issue the following command:

   ```
   ./UnixInstallScript
   ```

   The Check Point master installer starts to run.

3. Read the master installer welcome screen and type **N** (for Next).

4. Read the license agreement and type **Y** to accept.

5. Select **Check Point Enterprise / Pro** and type **N**.

6. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and type **N**.

7. When the product menu appears, choose **SmartCenter** by typing the corresponding number. Then type **N** to continue.

   Note that SmartConsole does not run on Linux. To use SmartConsole with a SmartCenter installation on Linux, you must install SmartConsole on separate Windows host. (For details on installing SmartConsole, see "Installing SmartConsole components," on page 45.)

8. Select **Primary SmartCenter** and type **N**.

9. When the Validation screen appears, verify the installation settings and type **N**.

   The SmartCenter installer runs, requiring no user input. When the SmartCenter installer completes, the Check Point configuration program launches automatically.

10. Perform basic configuration steps with the Check Point configuration program. For details, see "The Check Point Configuration Tool," on page 51.

11. Type **E** to exit the master installer.

Check Point SecurePlatform (Command Line Version)

To install SmartCenter in a distributed installation:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.

2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see "Installing Check Point SecurePlatform," on page 45.

   Run the cpconfig command to start the installer.

3. Read the master installer welcome screen and type **N** (for Next).
4. Read the license agreement and type **Y** to accept.
5. Select **Check Point Enterprise / Pro** and type **N**.
6. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and type **N**.
7. When the product menu appears, choose **SmartCenter** by typing the corresponding number. Then type **N** to continue.

   Note that SmartConsole does not run on SecurePlatform. To use SmartConsole with a SmartCenter installation on SecurePlatform, you must install SmartConsole on a separate Windows host. (For details on installing SmartConsole, see "Installing SmartConsole components," on page 45.)
8. Select **Primary SmartCenter** and type **N**.
9. When the Validation screen appears, verify the installation settings and type **N**.

   The SmartCenter installer runs, requiring no user input. When the SmartCenter installer completes, the Check Point Configuration Tool launches automatically.
10. Perform basic configuration steps with the Check Point Configuration Tool. For details, see "The Check Point Configuration Tool," on page 51.
11. Type **E** to exit the master installer.
12. Press **Enter**, log out by exiting the master installer (type **exit** and press **Enter**, two times), and then log in again to complete the installation. You can now start the SmartCenter by running **cpstart**.
13. Restart the computer.

Check Point SecurePlatform (GUI Version)

To install SmartCenter in a distributed installation:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.
2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see "Installing Check Point SecurePlatform," on page 45.
3. Using Internet Explorer, navigate to https://<SPLAT IP>:<Port number>.

   If you are prompted to allow popups, allow them always for this site. The welcome page appears.
4. Click **Next** to continue. In the subsequent pages you will have the opportunity to configure the following:

   - Network Connections

- Routing Tables
- DNS Servers
- Host and Domain Name
- Device Date and Time
- Web/SSH Clients

You may configure any of these you wish, or skip them, depending on your installation needs. Use the **Next** button to proceed through the pages until you reach the **Installation Options** page.

5. Select **Check Point Enterprise / Pro** or **Check Point Express** and click **Next**.
6. Select **SmartCenter**, making sure to deselect any other default selections, and click **Next**.
7. Select **Primary SmartCenter** and click **Next**.
8. The Smart Center configuration begins.

   Use the **Next** button to proceed through the configuration pages, entering your information. For more information about these options, see "Configuration tool options," on page 52.
9. Click **Finish** to finish the installation.
10. Confirm the installation. When the installation and configuration process finishes, reboot your computer.

Integrity and Provider-1

This section describes how to install Integrity Advanced Server with Check Point Provider-1 in an integrated installation. This release supports the integration of a single Integrity Advanced Server (either multi- or single-domain) with one Customer Management Add-On (CMA) in a Provider-1 environment. Note that, when setting up a distributed installation, you can install Integrity and Provider-1 on different operating systems.

The following topics are covered:

- "Provider-1 Overview," on page 41
- "Installing Integrity and Provider-1," on page 42

Provider-1 Overview

Provider-1 is a security solution designed to manage firewalls (in this case, Check Point VPN-1 gateways) for many widely-distributed networks. The networks may belong to different corporate branches, different customers, or even different companies. Provider-1 lets administrators create security policies centrally and then distribute them automatically to multiple firewalls.

Administrators manage firewalls through Customer Management Add-Ons (CMAs). A CMA is the equivalent of a standalone SmartCenter server in the VPN-1 Pro model (see the *VPN Guide* and *Firewall and SmartDefense Guide*). Unlike SmartCenter, however, CMAs reside on a centralized management node called a Multi-Domain Server (MDS). In addition to CMAs, the MDS also contains all Provider-1 system information. Though an MDS may contain many CMAs, each CMA is completely isolated from the others, providing absolute privacy for the department, customer, or company.

The Multi-Domain GUI (MDG) is the central management console for the entire Provider-1 environment.

For complete information about Provider-1, see the *Provider-1/SiteManager-1 User Guide*.

Installing Integrity and Provider-1

To install Integrity and Provider-1:

1. Install Provider-1. See the *Provider-1/SiteManager-1 User Guide*.
2. Install SmartConsole and MDG (the Provider-1 GUI) together on one host. See the *Provider-1/SiteManager-1 User Guide*.
3. Install Integrity Advanced Server by doing one of the following:
   - If you are installing Integrity on a host other than the Provider-1 host, follow the instructions in "Installing Integrity on a dedicated host," on page 25.

   > The Integrity Advanced Server host and the Provider-1 host must be set to the same time zone.

   - If you are installing Integrity on the same host as Provider-1, follow the instructions in "Installing Integrity on the same host as Provider-1," on page 42.
4. Configure the communication between Integrity and the Provider-1 CMA. To do so:
   a. In MDG (the Provider-1 GUI), create a new customer. Under the customer, create a CMA object. For details on creating customers and CMA objects in MDG, see the *Provider-1/SiteManager-1 User Guide*.
   b. Create an Integrity object in SmartDashboard. For details, see "Connecting Integrity and Provider-1," on page 43.

Installing Integrity on the same host as Provider-1

This section explains how to install Integrity on the same host as Provider-1.

To install Integrity on the Provider-1 host:

1. Log in as root to the Provider-1 host. Change directories from the MDS environment to the desired CMA environment by issuing the following command:

```
mdsenv <cma_name>
```

2. Change the permissions on the `ISSetup.bin` file.

```
[root@localhost /usr/local] chmod +x ISSetup.bin
```

3. Run the `ISSetup_X_X_XXX_X.bin` file.

   The Integrity Advanced Server Installer starts.

4. Follow the instructions in the wizard, entering the information for your installation. To go back to a previous step in the installer, type ‘back’. For information on completing the installation, see “The Integrity Advanced Server installer,” on page 47.

   Upon installation, the Integrity installer automatically picks up the CMA’s IP address.

Connecting Integrity and Provider-1

To establish communication between Integrity and Provider-1, ensure that SmartDashboard includes an Integrity Advanced Server object. (An Integrity object represents Integrity Advanced Server in SmartDashboard.) You must configure the Integrity object by following the instructions below. For detailed instructions on using SmartDashboard, see the *SmartCenter User Guide*.

To configure an Integrity object:

1. Log in to SmartDashboard.
2. Right-click the Check Point object in the navigation panel, and choose **New Check Point I Host...**.

   The Check Point Host dialog box appears.

3. In the dialog box, type the name and IP address of the Integrity Advanced Server host.
4. Click **Communications**, type the activation key you created after installing Integrity Advanced Server, and then click **Initialize**.
5. Select **Integrity Server** from the **Product** list and click **OK**.

   The new Integrity object appears under the Check Point node in the navigation panel.

6. In the menu bar, select **Policy I Install Database** to install the database.

   The Install Database dialog box appears, showing the Provider-1 CMA.

7. Click **OK**.

   The CMA installs the policy and database. When the installation completes, the dialog box displays the message, “Database installation succeeded.”

8. Click **Close** to close the Install Database dialog box.
9. Save your changes to SmartDashboard. (For example, select **File l Save**.)

You can now access the IAS administration console from SmartDashboard. To do so, right-click the Integrity object and choose **Manage Integrity Server**.

Installing SmartConsole components

SmartConsole is Check Point's suite of user interfaces. If you install Integrity with SmartCenter, you must also install SmartDashboard, the SmartCenter management UI included in SmartConsole. It is recommended to install SmartDashboard on a host other than those running Integrity and/or SmartCenter. SmartConsole (which includes SmartDashboard) runs on Windows, but not on Linux or SecurePlatform.

To install SmartConsole:

1. On the intended Windows computer, double-click the setup.exe file.

   The Check Point master installer begins.

2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. Choose **Check Point Enterprise / Pro** and click **Next**.
5. Choose **New Installation** and click **Next**.
6. Choose **SmartConsole**, making sure to deselect any other default selections. Click **Next**.
7. Click **Next** to start the installation.

   The master installer automatically launches the SmartConsole installer. This may take a couple minutes.

8. Specify the installation directory or accept the default, and click **Next**.
9. Select the UI client applications to install or accept the defaults, and click **Next**.
10. When prompted to create desktop shortcuts, click **Yes** or **No**, as desired.
11. When prompted to confirm the successful installation, click **OK** and then click **Finish**.
12. When the master installer reappears, click **Finish**.

Installing Check Point SecurePlatform

SecurePlatform is Check Point's secure version of Linux. For security purposes, it includes only a subset of Linux functionality. This section briefly describes how to install the SecurePlatform operating system, highlighting the steps required for a subsequent installation of Integrity Advanced Server on the same host. For more detailed information about SecurePlatform, see the Check Point *Getting Started Guide* and the *SecurePlatform Pro & Advanced Routing Command Line Interface Guide*.

The IAS installer is bundled with the appropriate SecurePlatform installer (along with the installers for any other Check Point products you plan to integrate with IAS) on one installation CD. Always install the version of SecurePlatform that is on the same CD as the IAS version you plan to use. When you run the master installer, it first guides you through the installation and configuration of SecurePlatform. It then launches, in sequence, the installers for Integrity Advanced Server and any other Check Point products you choose. The master installer concludes by running the Check Point Configuration Tool. If you quit the master installer before completing all desired configuration steps, you can return later and launch the configuration tool from the command line. If you quit the installer while it is still installing, you will have to run the installer again from the beginning.

If you are installing IAS with other Check Point products and you plan to use SmartConsole to administer the installation, you must install SmartConsole on a separate computer. SmartConsole does not run on SecurePlatform.

To install SecurePlatform:

1. Insert the SecurePlatform master installation CD and reboot from the CD to start the installer.

   The welcome screen appears.

2. Press **Enter**.

   The SecurePlatform installation wizard begins, prompting you (in sequence) to add device drivers, to decide which system type to install, to enter an IP address, to configure the HTTPS connection, and so on. (For detailed information on these options, see the Check Point *Getting Started Guide* and the *SecurePlatform Pro & Advanced Routing Command Line Interface Guide*.)

3. Work through the wizard, choosing the options appropriate for your installation. In the process, make sure to do the following:

   a. In the Network Interface Configuration screen, define the IP address, netmask, and default gateway. You must use a static IP address.

   b. In the HTTPS Server Configuration screen, change the port from the default. You must change this port if you are installing Integrity Advanced Server, because the default port number is already used by IAS. For example, change the port number to 9443.

4. Before confirming the installation, note that it will erase all existing information on the computer. If this is acceptable, click **OK**.

   The SecurePlatform installer takes several minutes to format the hard drive and upload the available product installation packages. When the installer finishes, it prompts you to restart the computer.

5. Click **OK** to restart the computer. Remove the CD. (Most computers eject the CD automatically at shutdown.)

   SecurePlatform starts up in “normal mode” by default.

6. Log in with username **admin** and password **admin**. When prompted, enter a new password. Optionally, you can specify a different user name, or press **Enter** to keep the current user name.

7. At the [cpmodule]# prompt, type **expert** and press **Enter**. Enter your password and then create an expert password.

   You are now in expert mode, which provides more configuration options.

8. Type **cpconfig** and press **Enter**, and then type **n** and press **Enter**.

   You now have the option of configuring, modifying, or confirming the host name, the domain name, the domain name servers, the network connections, and the routing. To choose a configuration option, type the corresponding number and press **Enter**. To return to the options menu, type **e** and press **Enter**. (For detailed information on these options, see the Check Point *Getting Started Guide* and the *SecurePlatform Pro & Advanced Routing Command Line Interface Guide*.)

9. When you finish the network configuration, type **n** and press **Enter**.

   You now have the option of setting the date and time.

10. When you finish the date and time configuration, type **n** and press **Enter**.

    You now have the option of fetching an import file from the TFTP server.

11. When you finish with the TFTP screen, type **n** and press **Enter**.

    The master installer starts. If you are installing SecurePlatform in conjunction with other Check Point products, return to the instructions appropriate for your installation.

The Integrity Advanced Server installer

Use the following information to complete the IAS installation wizard.

Installation Types

The installers give you a choice of the following installation types:

- **New Installation**—Use this option to install Integrity Advanced Server without clustering or to set up the first server in a cluster.

- **Import data from existing Integrity 5.x system**—Use this option to import data from an Integrity 5.x server after a successful installation. You will be prompted for import information after logging into the newly-installed system..

- **Join Cluster**—Use this option to install Integrity Advanced Server for joining with an existing cluster.

Server Type

There are two server types:

- **Integrity Advanced Server**—Choose this option if you want clustering. Integrity Advanced Server can function as either a single or multiple domain installation.
- **Integrity Server** —Choose this option for a single domain installation without clustering.

Server Properties

Enter the properties for your local server.

- **Local Host IP Address**—Enter the IP address or host name of the local computer the server will run on. If the computer has multiple NIC cards, you must provide an IP address for the NIC card you use.

If you use an IP address instead of a host name, you will not be able to change the IP address.

- **External Host IP Address**—Enter the external IP address used by the Integrity clients to connect to the server. If this is to be a clustered installation, the IP address can be the load balancer's IP address.
- **External Host Name**—Enter the host name that maps to the external IP address. This field is used in browser URLs and to create the certificate. This field can be the IP address.
- **Heartbeat port**—Enter the UDP heartbeat port.

Domain Options

- **Single Domain**—Single domain Integrity Advanced Server installations can only have one domain segment for all administrators, user directories, and policies
- **Multiple Domains**—Multiple domain Integrity Advanced Server installations can have multiple data segments for different administrators, user directories, and policies. You can use this feature to create virtual grouping for users to reflect company branches, sub-organizations, etc. Each domain can have its own security policies and system administrators can assign local administrators to each domain.

Clustering Options

- **Enable Clustering**—Choose this option to enabled clustered installation with multiple servers.

If you intend to use clustering and have only one server you can enable this option now and install additional servers later.

> If you wish to cluster your Integrity Advanced Servers, you must contact your Check Point representative for special instructions.

Clustering Information

Use the following information to complete the clustering information for your implementation.

- **Clustering Multicast Addresses**—These addresses are used for session replication and server to server communication in a cluster. Multicasting allows the servers to find each other dynamically in a cluster. Valid addresses are in the range: 224.0.0.0 to 239.255.255.255. The default is usually sufficient.
- **Clustering Ports**—These ports are used on the servers for multicasting.

Database Information

The Integrity Advanced Server uses a database to store operational and log information. Use the following information to specify the information for the database.

- **Database Type**—Select a database type.

> Note that when using the SPLAT GUI installer, you must use the embedded database.

- **JDBC Driver Folder**—Enter the location of the JDBC drivers residing locally on your server. If you do not already have the driver files, see“Obtaining the driver files,” on page 49.
- **Database Name**—Enter the name of the database instance. See “Configuring the databases and gathering information,” on page 22 for more information about specific databases.
- **Host Address**—Enter the host address of the database server.

> Use a host name rather than an IP address to specify your database. This allows you to later change your database.

- **Port Number**—Enter the port number of the database server.
- **Username**—Enter the username you use to access the database.
- **Password**—Enter the password you use to access the database.

Obtaining the driver files

Obtain the necessary driver files for your database type.

Obtaining the Oracle 9i driver files

You must download and install the Oracle 9i JDBC (Java Database Connectivity) drivers. These drivers are available free of charge from the Oracle Web Website. You will need an Oracle Technology Network account to download the drivers. This account is available for free.

To download the Oracle 9i drivers:

1. Using a Web browser, go to the Oracle 9i JDBC driver page.
2. In the 'For use with JDK 1.4' section, click the link for ojdbc14.jar.
3. Save the ojdbc14.jar file on the computer you wish to install Integrity Server on. Be sure to note the location.

Obtaining the Microsoft SQL Server 2000 driver files

You can download and install the Microsoft SQL Server 2000 JDBC (Java Database Connectivity) drivers free of charge from the Microsoft SQL Server page.

To download the Microsoft SQL Server 2000 drivers:

1. Using a Web browser, go to the Microsoft SQL Server download page.
2. In the 'Tools and Utilities' section, click SQL Server 2000 Driver for JDBC.
3. Follow the instructions for your operating system. Be sure to choose the Complete Setup option in the setup wizard.

   The Microsoft SQL Server 2000 drivers are stored by default in C:\program files\microsoft sql server 2000 driver for jdbc\lib.

Setting Client Languages

During installation, you can choose which languages (other than English) are available for Integrity communications with the endpoint user (such as client-package messages, custom alerts, and remediation or sandbox pages). The administrator will be able to use any of the selected languages for such communications.

To add client language options *after* installation:

1. Shut down Integrity Advanced Server. At the command line, go to <install_dir>\engine\webapps\ROOT\bin.For Windows, run the following:

   installLocale <locale>

   For Linux, run the following:

   ./installLocale.sh <locale>

   —where <locale> is ja_JP (for Japanese), fr_FR (for French), or de_DE (for German).

Do not try to install a language with this script if you have already installed that language.

Completing the installation

When the installation is complete, you will be given the option of starting the services and launching the Administrator Console. (This option is only available in the Windows Installer). You can launch the Administrator Console at any time by entering the Administrator Console URL in a supported browser: http://<Integrity Advanced Server IP Address>/signon.do.

The default login for the Integrity Advanced Server is 'masteradmin' and the default password is 'password'. If you are using RADIUS authentication, enter the password you used for the RADIUS server for this account. You will be prompted to change your password the first time you log in.

If you integrate Integrity Advanced Server with SmartCenter, note that an administrator can use the SmartCenter administrator role (created during initial SmartCenter configuration) to access IAS through SmartCenter.

Integrity prompts you to change your password periodically. Passwords must be at least six characters long.

Initial configuration of Check Point products

This section explains initial configuration of Check Point products, highlighting steps that are necessary when IAS is part of the installation.

The following topics are covered:

- "The Check Point Configuration Tool," on page 51
- "Connecting Integrity and SmartCenter," on page 53
- "Configuring VPN-1 Firewall to allow access to Integrity," on page 54

The Check Point Configuration Tool

Use the Check Point Configuration Tool (cpconfig) to perform basic configuration options, such as installing local licenses, creating a SmartCenter administrator, and so on.

The following topics are covered:

- "Starting the configuration tool," on page 52
- "Configuration tool options," on page 52

Starting the configuration tool

The configuration tool launches automatically after you install any Check Point product, including Integrity Advanced Server. You can also start the configuration tool manually, as described below.

To start the configuration tool manually:

➮ On SecurePlatform or Linux, go to the command line and issue the command **cpconfig**. On Windows, go to **Start | All Programs | Check Point SmartConsole | Check Point Configuration** or use the **cpconfig** command in the command line interface.

Configuration tool options

This section briefly describes what you can do with the Check Point Configuration Tool, highlighting features that are especially useful for an environment that includes Integrity Advanced Server. For detailed information about the configuration tool, see the Check Point *Getting Started Guide* and the configuration tool's associated online help.

Use the configuration tool to configure:

- **Local Licenses**—You can retrieve, add, and delete licenses for use on the current host. If you choose not to enter a license at installation, the configuration tool activates a 15-day trial license automatically. For further license management (including creating centralized licenses or licenses for other computers), use SmartUpdate. For more information about licenses, see "Licensing," on page 60.
- **The SmartCenter Administrator (required)**—You must create a SmartCenter administrator role that is used for single sign-on to all Check Point products.

  The SmartCenter administrator credentials let you log into SmartConsole, from which you can access the Integrity Advanced Server administrator console. Note that the first time an administrator logs into IAS directly (that is, *not* through SmartConsole), he or she can access the console using the out-of-the-box master administrator credentials (user name "masteradmin" and password "password").
- **GUI clients**—GUI clients are remote SmartConsole installations from which administrators can connect to the SmartCenter Server. If you do not define at least one GUI client, you will only be able to administer SmartCenter from a GUI client on the SmartCenter Server host itself.

  You can define remote clients by specifying their hostnames or IP addresses. Acceptable formats are IP address (for example, 1.2.3.4), IP address and netmask (1.2.3.4/255.255.255.0), IP range (1.2.3.4 - 1.2.3.20, or 1.2.3.*), or hostname (alice.checkpoint.com). Alternatively, you can type "Any" (without quotation marks) to allow access to all remote clients. The remote computers must be running SmartConsole.
- **Certificate Authority (required)**—You must initialize a certificate authority to enable communication between Check Point components. To do so, specify a host

name in the format <hostname>.<domain_name> (for example, alice.checkpoint.com).

For SecurePlatform installations, the configuration tool handles this automatically.

- **Secure Internal Communication (required on the IAS host in a distributed installation)**—When you use the master installer to install Integrity Advanced Server on a different host than SmartCenter, you must create an activation key that will be used to secure communication between IAS and SmartCenter. Make note of the activation key, because you will need it when configuring an Integrity object in SmartDashboard. (For details on configuring an Integrity object, see "Connecting Integrity and SmartCenter," on page 53.)
- **Fingerprint (Required)**—The configuration tool creates a fingerprint (a text string derived from the SmartCenter certificate), which you use to verify the identity of the SmartCenter Server the first time you log in to SmartConsole. You can export the fingerprint to a file and provide it to administrators. Administrators should make sure that this fingerprint matches the one displayed the first time SmartConsole connects to the SmartCenter Server.

Connecting Integrity and SmartCenter

To establish communication between Integrity and SmartCenter, ensure that SmartCenter (SmartDashboard) includes an Integrity Advanced Server object. (An Integrity object represents Integrity Advanced Server in SmartCenter.) When you install both Integrity Advanced Server and SmartCenter on the same host, the installer creates the object automatically. If you are setting up a distributed installation (IAS on one server, SmartCenter on another), you must configure the Integrity object manually by following the instructions below. For detailed instructions on using SmartDashboard, see the *SmartCenter User Guide*.

To configure an Integrity object:

1. Log in to SmartDashboard using the SmartCenter credentials you configured with the Check Point Configuration Tool.
2. Right-click the Check Point object in the navigation panel, and choose **New Check Point I Host...**.

   The Check Point Host dialog box appears.
3. In the dialog box, type the name and IP address of the Integrity Advanced Server host.
4. Click **Communications**, type the activation key you created after installing Integrity Advanced Server, and then click **Initialize**.

   The **Trust State** field should show **Trust Established**. If it does not, reset and create the SIC again.
5. Select **Integrity Server** from the scrolling list and click **OK**.

   The new Integrity object appears under the Check Point node in the navigation panel.

6. In the menu bar, select **Policy | Install Database** to install the policy and database.

   The Install Database dialog box appears, listing the primary SmartCenter Server and any other SmartCenter Servers.

7. Click **OK**.

   SmartCenter installs the policy and database. When the installation completes, the dialog box displays the message, “Database installation succeeded.”

8. Click **Close** to close the Install Database dialog box.

9. Save your changes to SmartDashboard. For example, select **File | Save**.

You can now access the IAS administration console from SmartCenter. To do so, right-click the Integrity object and choose **Manage Integrity Server**.

Configuring VPN-1 Firewall to allow access to Integrity

In order to use Integrity Advanced Server with VPN-1, you must be sure that VPN-1 is not blocking traffic to and from Integrity Advanced Server. Configure your VPN-1 Firewall to allow the following traffic:

Outbound

Table 4-1: Outbound Traffic

Port	Protocol
443	HTTPS

Inbound

Table 4-2: Inbound Traffic

Port	Protocol
80	TCP
443	TCP
4433	TCP
6054	UDP
8009	TCP
8010	TCP

Optional outbound

Allow the following traffic as needed by your installation.

Table 4-3: Optional outbound traffic

Use	Port	Protocol
LDAP	389	TCP
RADIUS	1812	UDP
ZSP (with Cisco Concentrator)	5054	TCP
NetBIOS	137, 138, and 139	TCP
SQLServer	1433	TCP
Oracle	7777	TCP
DB2	50000	TCP
NTP	123	TCP

For more information about how the Integrity Advanced Server communicates with other products and devices, see the ***Integrity Advanced Server Installation*** guide. If you change these ports, you must allow traffic on the new ports.

Remote logging

You may want to install and configure the log server on a separate host for remote logging. This section explains how to set up remote logging for most installations, including Integrity standalone, Integrity and SmartCenter on the same host, and Integrity and SmartCenter on separate hosts. For complete details on all configuration options, see the Check Point *Getting Started Guide* and the *SmartCenter Guide*.

The following topics are covered:

- "Installing the log server remotely," on page 55
- "Configuring remote logging," on page 59

Installing the log server remotely

This section describes how to install the log server on a separate host.

Windows

To install a log server on Windows:

1. On the intended host server, double-click the setup.exe file.

   The Check Point master installer begins.

2. Click **Next**.
3. Accept the license agreement and click **Next**.
4. Choose **Check Point Enterprise / Pro** and click **Next**.
5. Choose **Demo Installation**, **New Installation**, or **Installation Using Imported Configuration**, as appropriate, and click **Next**.
6. Choose **SmartCenter** (making sure to deselect any other defaults) and click **Next**.
7. Choose **Log Server** and click **Next**.
8. Click **Next** to start the installation.

   The Installation Status bar appears, displaying the chosen installation package. The master installer automatically launches the installer for the selected product.
9. Specify the installation directory or accept the default, and click **Next**.

   The installer begins. It may take a couple minutes.
10. When the SmartCenter installer completes, click **OK**.

    The installer performs configuration in the background for up to five minutes. Do not interrupt the configuration, even if it appears as if nothing is happening. When the installer finishes, it launches the Check Point Configuration Tool.
11. Perform basic configuration steps with the Check Point Configuration Tool. For details, see "The Check Point Configuration Tool," on page 51.
12. Click **Finish** in the master installer, and then restart the computer.
13. Complete the configuration steps described in "Configuring remote logging," on page 59.

Linux

To install a log server on Linux:

1. On the intended host server, go to the installer directory and issue the following command:

   ```
   ./UnixInstallScript
   ```

   The Check Point master installer starts to run.

2. Read the master installer welcome screen and type **N** (for Next).
3. Read the license agreement and type **Y** to accept.
4. Select **Check Point Enterprise / Pro** and press **N**.
5. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and press **N**.
6. When the product menu appears, choose **SmartCenter** by typing the corresponding number. Then type **N** to continue.
7. When prompted to specify the SmartCenter installation type, choose **Log Server** and type **N**.
8. When the Validation screen appears, verify the installation settings and type **N**.

   The SmartCenter installer begins. When the SmartCenter installer completes, the Check Point Configuration Tool launches automatically.
9. Perform basic configuration steps with the Check Point Configuration Tool. For details, see "The Check Point Configuration Tool," on page 51.
10. Type **E** to exit the master installer.

Check Point SecurePlatform (Command Line Version)

When installing IAS on SecurePlatform, install the version of SecurePlatform that corresponds to the IAS version you plan to install. The appropriate SecurePlatform version is included on the installation CD.

To install a log server on SecurePlatform:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.
2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see "Installing Check Point SecurePlatform," on page 45.

   In Windows and Linux installations, when the SecurePlatorm installer completes, the Check Point master installer launches automatically.

   For SPLAT installations, you need to run the cpconfig command to start the installer.

3. Read the master installer welcome screen and type **N** (for Next).

4. Read the license agreement and type **Y** to accept.

5. Select **Check Point Enterprise / Pro** and type **N**.

6. Select the appropriate option (**New Installation** or **Installation Using Imported Configuration**) and type **N**.

7. When the product menu appears, choose **SmartCenter** by typing the corresponding number. Then type **N** to continue.

8. When prompted to specify the SmartCenter installation type, choose **Log Server** and type **N**.

9. When the Validation screen appears, verify the installation settings and type **N**.

   The SmartCenter installer begins. When the SmartCenter installer completes, the Check Point Configuration Tool launches automatically.

10. Perform basic configuration steps with the Check Point Configuration Tool. For details, see "The Check Point Configuration Tool," on page 51.

11. Type **E** to exit the master installer.

12. Press **Enter**, log out by exiting the master installer (by typing **exit** and pressing **Enter**, and then repeating), and then log in again to complete the installation. You can now start the installed product by running **cpstart**.

Check Point SecurePlatform (GUI Version)

When installing IAS on SecurePlatform, install the version of SecurePlatform that corresponds to the IAS version you plan to install. The appropriate SecurePlatform version is included on the installation CD.

To install a log server on SecurePlatform:

1. Insert the CD and reboot from the CD to start the installer.

   The installer begins by guiding you through the installation of the SecurePlatform operating system.

2. Complete the installation wizard for the SecurePlatform operating system. For details on installing SecurePlatform, see "Installing Check Point SecurePlatform," on page 45.

3. Using Internet Explorer, navigate to https://<SPLAT IP>:<Port number>.

   Use the port number you specified during the installation of SecurePlatform. If you are prompted to allow popups, allow them always for this site. The welcome page appears.

4. Click **Next** to continue. In the subsequent pages you will have the opportunity to configure the following:

   - Network Connections

- Routing Tables
- DNS Servers
- Host and Domain Name
- Device Date and Time
- Web/SSH Clients

You may configure any of these you wish, or skip them, depending on your installation needs. Use the **Next** button to proceed through the pages until you reach the **Installation Options** page.

5. Select **Check Point Enterprise / Pro** or **Check Point Express** and click **Next**.
6. Select **SmartCenter** or **SmartCenter Express** and click **Next**.
7. When prompted to specify the SmartCenter installation type, choose **Log Server**
8. The Check Point Configuration Tool launches automatically.
9. Use the **Next** button to proceed through the configuration pages, entering your information. For more information about these options, see "Configuration tool options," on page 52.
10. Click **Finish** to finish the installation.
11. Confirm the installation. When the installation and configuration process finishes, reboot your computer.

Configuring remote logging

This section describes how to configure a remote log server in SmartDashboard. The instructions, which assume that you have already installed Integrity Advanced Server on another host, are valid for all supported operating systems.

Follow the instructions in each of the following sections:

- "Connecting the log server and SmartCenter," on page 59
- "Connecting the log server and Integrity," on page 60

Connecting the log server and SmartCenter

To establish communication between a remote log server and SmartCenter, you must create a log server object in SmartDashboard. To do so, follow the directions below.

To create a log server object:

1. Log in to SmartDashboard.
2. Right-click the Check Point object in the navigation panel, and choose **New Check Point I Host...**.

   The Check Point Host dialog box appears.

3. In the dialog box, type the name and IP address of the log server host.
4. Click **Communications**, type the activation key you created after installing the log server, and then click **Initialize**. When a message appears indicating that trust is established, click **Close**.
5. Select **Log Server** from the Check Point Products list and click **OK**.

   The new log server object appears under the Check Point node in the navigation panel.

Connecting the log server and Integrity

To establish communication between a remote log server and Integrity, you must configure the Integrity object in SmartDashboard. To do so, follow the directions below.

To configure the Integrity object:

1. In SmartDashboard, right-click the Integrity object and select **Edit**.

   The Check Point Gateway dialog box appears.
2. If you have not defined a log server, click on the **Log Servers** node in the navigation panel. In the dialog box that appears, configure the log server settings for your installation.

   If you have already defined a log server, continue to step 3.
3. Click on the **Additional Logging** node in the navigation panel, and do the following:
   a. Select Forward log files to SmartCenter server and choose the desired log server from the dropdown list.
   b. Set any other desired parameters.
   c. Click **OK**.
4. On the menu bar, select **Policy | Install Database...** to register your modified SmartDashboard objects.

Licensing

Check Point requires licenses for Security Gateways, SmartCenter Server, and Integrity Advanced Server. SmartConsole does not require a license. Add-on licenses are required for some special features, such as Integrity Advanced Server's Program Advisor.

Each Check Point product comes with a trial license that allows unrestricted use of the product for 15 days. Trial licenses include all product features.

For complete details on all licensing options and enforcement behaviors, contact your Check Point representative.

This section covers the following topics:

Licenses for Integrity Advanced Server

All installations require an Integrity client license, which allows you to run Integrity clients on your endpoints. Optionally, you can also purchase licenses for special Integrity features. The following licenses are available for Integrity Advanced Server:

- **Integrity clients**—Permits a specified number of endpoints to run the Integrity client. This license is required.
- **IM Security**—Permits a specified number of endpoints to use Integrity IM Security.
- **Program Advisor**—Permits Integrity Advanced Server to receive the latest Program Advisor updates. The license is good for an unlimited number of endpoints.
- **Anti-Spyware (endpoints)**—Permits a specified number of endpoints to use Integrity Anti-Spyware.
- **Anti-Spyware (updates)**—Permits Integrity Advanced Server to receive the latest Anti-Spyware updates.

Using licenses

You must install and attach Integrity licenses with one of the Check Point license management tools: SmartUpdate, the cplic command, or (for local licenses only) the Check Point Configuration Tool. (For information on these options, see "Attaching licenses," on page 62.)

After a feature has been enabled on Integrity Advanced Server, you can incorporate that feature into security policies, which you can then deploy to Integrity clients. An endpoint's active policy controls which features are enabled on that endpoint.

Expired or exceeded licenses

For the Integrity Clients license, the Integrity Advanced Server checks for the maximum number of endpoints that connected during the last 24 hours. This check runs every 24 hours after the server starts. If your installation exceeds the number of allowed endpoints, the Integrity Advanced Server goes into read-only mode. Your endpoints are still protected by their existing policies, but you will be unable to make changes until you enter your new license through Smart Update. Contact your Check Point representative to get a new license and restore editing privileges.

While you are waiting for your new Integrity Clients license, you can use a trial license. Contact your Check Point representative to obtain a trial license.

If a feature license expires, Integrity either disables editing privileges or prohibits administrator access to the feature.

Licensing your products

When licensing your products, decide whether to manage the licenses centrally or locally. The differences between central and local licensing are as follows:

- **Central licensing**—You use SmartUpdate or the cplic command to store licenses in a central repository on SmartCenter Server, and then to attach the licenses to the desired computers. Central licenses are not tied to an IP address, and therefore can be reassigned as necessary. This is the recommended form of license management, and it is especially useful for distributed installations.
- **Local licensing**—Each license is tied to the IP address of the computer on which it is installed. Licenses are attached either with SmartUpdate or (locally) with the Check Point Configuration Tool or the command-line interface. If the IP address of the licensed computer changes, you must generate a new license for that computer.

To license your products:

1. Generate the licenses. (See page 62.)
2. Attach the licenses. (See page 62.)

Generating licenses

Check Point provides certificate keys for each license you purchase. Use the certificate keys to generate licenses.

To generate a license:

1. Gather the following information:
   - Certificate key
   - Host IP address (For central licenses, use the SmartCenter Server host IP address.)
2. Log in to the Check Point User Center (www.checkpoint.com/usercenter) and navigate to the Getting Started page.
3. Follow the User Center instructions for generating a license.

Attaching licenses

Use SmartUpdate or the cplic command-line tool to attach licenses to your installations. Note that you must use one of these methods to install or update Integrity Advanced Server licenses, even if you are installing IAS by itself. For instructions on using SmartUpdate to attach the license, see the *SmartCenter User Guide*. For information on cplic, see the Check Point *Command Line Interface Guide*. You can also use the Check Point Configuration Tool to attach licenses locally. For information on the configuration tool, see “The Check Point Configuration Tool,” on page 51, the Check Point *Getting Started Guide*, and the configuration tool’s online help.

Configuring the RADIUS Server

The Integrity Advanced Server is configured by default to use its own administrator authentication method. If you wish to use a RADIUS server instead you will need to configure it now.

Prerequisites

Before beginning to configure your RADIUS server, make sure you have done the following:

- Record the RADIUS server host name or IP address and port (default port is 1812).
- Record your RADIUS server shared secret.
- Create an Integrity Advanced Server account, called “masteradmin” on the RADIUS server.

To configure the RADIUS server:

1. Perform the following steps to configure the RADIUS server. Configuration consists of updating a configuration file and a properties file. Update the configuration file.

   See “Updating the configuration file,” on page 63.

2. Configure the properties file.

   See “Configuring the properties file,” on page 64.

Updating the configuration file

To update the configuration file:

1. Shutdown the Integrity Advanced Servers.
2. Log in.

   SPLAT users should log in as ‘admin’. Windows users should log in as an administrator.

3. Go to the configuration file location.

   For Windows the default location is: \CheckPoint\Integrity\engine\webapps\ROOT\install\templates\config

   For Linux the default location is:

   /opt/CPIntegrity/engine/webapps/ROOT/install/templates/config

4. Create a backup of template-integrity-config.xml.
5. Open template-integrity-config.xml in a text editor.
6. In the AdminConsole node, remove the comment tags from the first RADIUS JAAS node, and remove the JAAS node for ‘inbuilt authentication of admin users’.
7. Save you changes and close the file.

   Make sure your XML is well-formed.

Configuring the properties file

To configure the properties file:

1. Go to the location of the properties file.

   For Windows, the default location is:

   CheckPoint\Integrity\engine\webapps\ROOT\install\templates.

   For Linux, the default location is:

   /opt/CPIntegrity/engine/webapps/ROOT/install/templates
2. Create a backup of install-upgrade.properties.
3. Open install-upgrade.properties in a text editor.
4. Specify the following properties:
   - radius.authtype=<CHAP or PAP>
   - radius.server=<IP address of your radius server>
   - radius.port=<Port for your radius server. Usually 1812.>
   - Radius.secret=<Radius secret code>
   - upgrade.from.version=<empty>
5. Save your changes and close the file.
6. Go to the utility location.

   For Windows, the location is:

   CheckPoint\Integrity\engine\webapps\ROOT\bin

   For Linux, the directory is:

   /opt/CPIntegrity/engine/webapps/ROOT/bin
7. Run the upgrade utility appropriate for your operating system:

- upgradeServer.bat (Windows)
- upgradeServer.sh (Linux).

8. Restart the Integrity Advanced Server.

Using Integrity with a proxy server

If you plan to use Integrity's Program Advisor feature or Anti-spyware feature in an environment that includes a proxy server for Internet access, perform the configuration steps below to let Integrity Advanced Server connect to Check Point's central servers (containing Program Advisor settings or Anti-spyware definitions) the through the proxy server. Note that all configuration entries are case-sensitive.

You do not have to perform this configuration at the time of installation. If desired, you can perform these steps when enabling Program Advisor or Anti-spyware. For information on Program Advisor, see Chapter 9, "Program Advisor," on page 127 in the *Integrity Advanced Server Administrator Guide*. For information on Anti-spyware, see Chapter 11, "Policies: Protecting Against Spyware," on page 149 in the *Integrity Advanced Server Administrator Guide*.

Configuration steps are are provided for the following operating systems:

- "Windows," on page 65
- "Linux," on page 65

Windows

To configure a proxy server:

1. Open the Registry Editor (regedit.exe).
2. Edit "My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0 \IntegrityTomcat\Parameters\Java\options" by adding the following:

```
-DproxySet=true
-Dhttp.proxyHost=hostname
-Dhttp.proxyPort=port
-Dhttps.proxyHost=hostname
-Dhttps.proxyPort=port
```

3. Close the Registry Editor.
4. Open the Services panel.
5. Stop the "Integrity Tomcat" service, and then restart it.

Linux

Follow the procedure that is appropriate for your installation.

To configure a proxy server (in a standard installation):

1. Edit `~/engine/bin/catalina.sh`, replacing the line:

   ```
   JAVA_OPTS="-Xms256M -Xmx512M -Djava.awt.headless=true"
   ```

   with the line:

   ```
   JAVA_OPTS="-Xms256M -Xmx512M -Djava.awt.headless=true -DproxyHost=true
   -Dhttp.proxyHost=hostname -Dhttp.proxyPort=port
   -Dhttps.proxyHost=hostname -Dhttps.proxyPort=port"
   ```

2. Save the file.
3. Restart Integrity by issuing:

   ```
   <Install Directory>/bin/IntegrityStop
   <Install Directory>/bin/IntegrityStart
   ```

   The default install directory is `/opt/CPIntegrity`

To configure a proxy server (if the JAVA_OPTS environment variable is already set):

1. Use the appropriate `setenv` call to reset the value of `JAVA_OPTS` to:

   ```
   "-Xms256M -Xmx512M -Djava.awt.headless=true -DproxyHost=true
   -Dhttp.proxyHost=hostname -Dhttp.proxyPort=port
   -Dhttps.proxyHost=hostname -Dhttps.proxyPort=port"
   ```

Updating the logo

If you want the Integrity Advanced Server user interface to display your company's logo, you must turn on cobranding and replace the image file with one of your logo.

To update the logo:

1. Log in as root.
2. Rename \CheckPoint\Integrity\engine\webapps\ROOT\css\zl-cobrandOff-css.css to \CheckPoint\Integrity\engine\webapps\ROOT\css\zl-cobrandOn-css.css
3. Replace the image file \Checkpoint\Integrity\engine\webapps\ROOT\images\misc\cobrand_logo.gif with a jpg or gif cobranded logo that is 180px in width and 63px in height.
4. If the image is not replaced, hold control and refresh your browser.

Uninstalling Integrity and other Check Point products

This section explains how to uninstall Integrity Advanced Server and other Check Point products. Refer to the instructions appropriate for your operating system.

Windows

To uninstall on Windows:

1. Go to **Start** | **Control Panel** | **Add or Remove Programs** and remove Integrity Advanced Server.
2. On the same computer, remove the Check Point software packages, making sure to remove the Check Point VPN-1 Pro component *last*, after removing all other Check Point software components.
3. If you have a distributed installation, access the SmartCenter host and go to the command line. Stop all Check Point services by running **`cpstop`**. Then go to **Start** | **Control Panel** | **Add or Remove Programs**. Remove the Check Point software packages, making sure to remove the Check Point VPN-1 Pro component *last*.

   Repeat this step for any other SmartCenter hosts in your configuration (for example, a separate host running a remote log server).

Linux

Follow the instructions below to uninstall Check Point software from a Linux system. On any host from which you are removing Check Point software, you must remove the `CPSuite-xxx-00` component (where `xxx` is the version number) *last*, after removing all other Check Point software components.

To uninstall from a Linux system:

1. Navigate to the uninstallation directory (by default, `/opt/CPIntegrity/Uninstall_Integrity`), and issue the following command:

   ```
   ./Uninstall_Integrity
   ```

   At the prompt, press **Enter**. The Integrity Advanced Server uninstallation wizard starts.
2. Work through the uninstallation wizard.
3. Issue the following command to see a list of Check Point components installed on your system:

   ```
   rpm -qa| grep CP
   ```

   Note that this command displays all software components containing “CP,” including some which are not Check Point components.

4. Issue the following command for each component to remove, making sure to remove the `CPSuite-xxx-00` component (where `xxx` is the version number) *last*:

   ```
   rpm -e <package_name>
   ```

5. If you have a distributed installation, access the SmartCenter host and run **`cpstop`**. Then repeat steps 3 and 4 on the SmartCenter host.

   Repeat step 5 for any other SmartCenter hosts in your configuration (for example, a host running a remote log server).

Check Point SecurePlatform

There is usually no reason to uninstall a Check Point product from a SecurePlatform host while leaving SecurePlatform intact. If you want to install a newer version of a Check Point product on SecurePlatform, it is recommended to back up your data and then reboot the host from the installation CD. Rebooting from the CD will remove SecurePlatform from the host and replace it with the version appropriate for your new installation. (Installation CDs for the SecurePlatform versions of Check Point products include the appropriate version of SecurePlatform for the installation.)

In rare cases, you may want to uninstall a Check Point product while leaving SecurePlatform intact. For example, if you are currently running Integrity and SmartCenter on one host, and you want to convert to a distributed installation (with Integrity and SmartCenter on separate hosts), you would back up your data and then uninstall Integrity or SmartCenter from the current host (without uninstalling SecurePlatform). In such cases, follow the instructions below.

To uninstall from a SecurePlatform system:

1. On the desired computer, stop all Check Point services by running **`cpstop`**.

2. To uninstall Integrity, navigate to the uninstallation directory (by default, `/opt/CPIntegrity/Uninstall_Integrity`), and issue the following command:

   ```
   ./Uninstall_Integrity
   ```

   At the prompt, press **Enter**. The Integrity Advanced Server uninstallation wizard starts.

3. Work through the uninstallation wizard.

   Remove Integrity Advanced Server.

   If you are removing only Integrity Advanced Server, this step completes the process.

4. Run the following command to see a list of Check Point components installed on your system:

   ```
   rpm -qa| grep CP
   ```

   Note that this command displays all software components containing “CP,” including some which are not Check Point components.

5. Run the following command for each component to remove, making sure to remove the `CPSuite-xxx-00` component (where `xxx` is the version number) *last*:

   ```
   rpm -e <package_name>
   ```

   You must remove Integrity before removing SmartCenter.

Chapter 3

Starting and Stopping Integrity Advanced Server

This chapter explains how to manually start, stop, and restart Integrity Advanced Server and the Apache httpd server.

For Integrity Advanced Server to operate, the database host and Integrity Advanced Server database instances must also be running.

The following instructions are found in this chapter:

Managing a Windows Setup

Stopping, starting, and resetting the services

Use the Control Panel to start, stop, or reset the Integrity Advanced Server, Apache, or Tomcat services.

To stop, start, or reset the services

1. Go to **Control Panel** | **Administrative Tools** | **Services**.
2. Right-click on the service and choose the option you want.

Managing a Linux Setup

Starting and stopping the Integrity Advanced Server

This section explains how to start and stop Integrity Advanced Server (only).

To start or stop Integrity Advanced Server only:

1. Log in to Integrity Advanced Server host as root.

   [root@localhost /] #

2. Run the start, stop, or restart shell:

   - Start: `<Install Directory>/bin/IntegrityStart`
   - Stop: `<Install Directory>/bin/IntegrityStop`

   The default install directory is `/opt/CPIntegrity`

Chapter 4

Setting Up System Event Logs

This chapter explains how to set up system event logging and provides recommended messaging and logs.

This chapter covers the following topics:

Understanding events and logging

Integrity Advanced Server produces log entries and messages in five formats: text, SMTP, SNMP, syslog, and JDBC. You can configure Integrity to direct messages to various destinations.

The preconfigured log and message types are:

- **Text** — Records event messages in a text file (on Integrity Advanced Server or any other accessible server). Messages are appended as the events occur.
- **SMTP** — Sends an event message to an SMTP destination, such as e-mail or a pager. Messages are sent as the events occur.
- **SNMP trap** — Sends an event message to a SNMP Manager. Messages are sent as the events occur.
- **Syslog** — Records events in a syslog file (on Integrity Advanced Server or a system log server). Messages are appended to the system log file as the events occur.
- **JBDC** — Sends events to a database configured on the same server as the Integrity main and log databases.

Recommended event logs

This section describes how to configure recommended event notifications. The following topics are covered:

- "Routing Fatal messages to e-mail and pager accounts (SMTP)," on page 75
- "Routing Log Upload System warn and error messages to e-mail and pager accounts (SMTP)," on page 76
- "Adding warn, error, and fatal messages to a system log (syslog)," on page 77

Routing Fatal messages to e-mail and pager accounts (SMTP)

Integrity Advanced Server generates Fatal events when immediate intervention is required to keep the system running or to bring the system back online. Use the following configuration to send Fatal messages to a list of e-mail recipients, including those with SMTP-compatible pagers.

To use this feature, you must be running an SMTP server through which Integrity can send messages.

Use the following settings to send Fatal event messages via SMTP.

Field	Setting	Description
Name	Fatal Events	Identifies the event to Integrity administrators.
Description	E-mail fatal event messages.	Describes the event type to Integrity administrators.
Type	SMTP	Formats the event message in the body of an e-mail.
Log Levels	Fatal	Specifies the type of event to send.
Event Classes	Select All	Select all ones you want to send to the receipt list. Note that you can set up separate recipient lists for different event types.
Server host	Host name or IP address of the SMTP mail server	Specifies the server Integrity will use to send messages.
Email from	Sender's e-mail address	Provides a contact for the recipient. It is recommended to use your Integrity support team's e-mail address.
Subject	E-mail subject line	Sets the e-mail subject line.

Field	Setting	Description
Recipients	Recipients' e-mail addresses	Identifies addresses to which to send messages. You can set up separate events for different groups.

Routing Log Upload System warn and error messages to e-mail and pager accounts (SMTP)

The Log Upload System loads client logs into the Integrity Advanced Server database. The Log Upload System does not produce any fatal errors for Integrity Advanced Server. However, critical information may be lost if this system fails.

> You may want to set up two events for the Log Upload System, one that sends warning level messages to administrators specifically assigned to the affected area, and another to broader group who would be affected by a complete failure.

This section explains how to send e-mail messages when the Log Upload System reaches a critical state.

Field	Setting	Description
Name	Log Upload System	Identifies the event to Integrity administrators.
Description	Critical messages from e-mail reporting system	Describes the event type to Integrity administrators.
Type	SMTP	Formats the event message in the body of an e-mail.
Log Levels	Warn and Error	Specifies the type of event to send.
Event Classes	Log Upload System	Specifies the type of message to send.
Server host	Host name or IP address of the SMTP mail server	Specifies the server Integrity will use to send messages.
Email from	Sender's e-mail address	Provides a contact for the recipient. It is recommended to use your Integrity support team's e-mail address.
Subject	E-mail subject line	Sets the e-mail subject line.
Recipients	Recipients' e-mail addresses	Identifies addresses to which to send messages. You can set up separate events for different groups.

Adding warn, error, and fatal messages to a system log (syslog)

By default, logging is set to the default `log4j` configuration in `integrity.xml`, which sends all logging to `integrity.log` in the `/usr/local/integrity/webapps/ROOT/logs` directory. Once Integrity Advanced Server is installed and running, it is recommended to create a general Syslog logging configuration that receives all these log events from the remote servers.

This section explains how to create a syslog that is stored on a host other than the Integrity Advanced Server host. Remember to configure the syslog server to listen for remote events, and to configure Integrity to send syslog events to the syslog server.

Field	Setting	Description
Name	System Log	Identifies the event to Integrity administrators.
Description	System status events.	Describes the event type to Integrity administrators.
Type	syslog	Causes Integrity to write events to a system log file.
Log Levels	Warn, Error, and Fatal	Specifies the types of events to log. It is recommended to log all these event types.
Event Classes	All	Specifies the types of events to log.
Server hostname	Host name or IP address of syslog server	Specifies the server Integrity will use to send messages. (For example, use `127.0.0.1` to store locally.)
Facility	USER	Enter the name of the syslog-facility handling Integrity Advanced Server event messages.

Using SNMP with Integrity

This section outlines the format of SNMP traps emitted by Integrity.

The following topics are covered:

- General Information
- Trap Formats

General Information

Set up an event destination to which to send SNMP traps. This is covered in "Creating and editing events," on page 79.

Trap Formats

Traps include a header and a message. All traps have a common header, as all are generated by Integrity Advanced Server. Here is an example trap showing administrator login:

```
[public]  [1.3.6.1.4.2620]  [enterprise]  [2734006]  [127.0.0.1]  [6]
[1234567]  [Ver1]  [1.3.6.1.4.1.2620.1.27.160]  [2005-08-23 14:47:12, 719,
INFO, [logInfoQueue-HQs:1] , [root] , [AdminLogin] Administrator Login,
ADMIN=masteradmin, SESSION_IP=209.87.212.91]
```

The trap header begins with `[public]` and ends with the event OID, `[1.3.6.1.4.1.2620.1.27.160]`. The message begins with the event time, `[2005-08-23 14:47:12]` and continues to the end of the trap.

Managing events

This section explains how to create, edit, and delete event logs and messages from Integrity Advanced Server.

Creating and editing events

This section provides the basic steps for accessing the Event Destination pages. See the associated online help for more information about specific event types, event classes, and log levels.

To create or edit an event:

1. Go to **System Configuration** | **Event Notification**.
2. Select the event and click **New** or **Edit**, as appropriate.

   The Edit Event Destination page appears.
3. Modify the information as desired and then click **Next**.

   A second Edit Event Destination page appears.
4. Change the location, or other details, and then click **Save**.

   The event is updated and the changes take effect immediately on the local host.

Deleting events

Deleting an event from Integrity Advanced Server completely removes it from the system. Integrity immediately stops recording and sending events from the local host.

To delete an event:

1. Go to **System Configuration** | **Event Notification**.
2. Select the event and click **Delete**.
3. Click **Yes** to confirm the deletion.

Chapter 5

Testing Integrity Advanced Server

Once you have installed and configured Integrity Advanced Server and started all the components, you are ready to set up Integrity Advanced Server for testing. Use the tests in this chapter to verify that:

- Integrity Advanced Server can detect a client session.
- Integrity Flex receives communications from Integrity Advanced Server and updates its enterprise policy.

To test the Integrity Advanced Server:

1. Set up the test environment.

   See “Setting up the Integrity Advanced Server test,” on page 81.

2. Perform the test.

   See “Performing the Integrity Advanced Server tests,” on page 84.

Setting up the Integrity Advanced Server test

Use the steps in this section to set up your system to test the basic functionality of Integrity Advanced Server.

For detailed instructions on using Integrity Advanced Server, refer to the *Integrity Advanced Server Administrator Guide*.

Perform the following steps:

1. Log on to the Integrity Advanced Server Administrator Console.

   See "Logging on to the Integrity Advanced Server Administrator Console," on page 81.

2. Create a user catalog.

   See "Creating a custom user catalog," on page 83.

3. Set up the endpoint computer.

   See "Setting up the endpoint computer," on page 83.

Logging on to the Integrity Advanced Server Administrator Console

The Integrity Advanced Server comes preconfigured with one administrator account, masteradmin. Note that, for installations that include SmartCenter and SmartDashboard, you can also log on to Integrity Advanced Server through SmartDashboard using the login credentials you created at installation.

If you are using a RADIUS server to authenticate, before you can use the account to log on, you must create it on that RADIUS server.

The masteradmin account has the highest level of permissions. Use this Administrator ID with the password you configured in the RADIUS server to log in for the first time.

To log on for the first time:

1. Open a browser, enter the Administrator Console URL.

```
http://integrityserverip/
```

If you are using Microsoft Internet Explorer and self-signed certificates the Security Alert prompt appears. See "Installing the security certificate," on page 82 to avoid seeing this prompt in future.

The Administrator Console login page appears.

2. For **Administrator ID**, enter ‘masteradmin’.
3. For **Password**, enter the appropriate password.
   a. If you are using the default, built-in authentication enter ‘password’.
   b. If you are using RADIUS authentication, enter the password you used for the RADIUS server for this account.
4. Click **Log in**.

   You are now logged into the Integrity Advanced Server Administrator Console.

Installing the security certificate

This step only applies to administrators with self-signed certificates that are using Internet Explorer.

To install the security certificate:

1. Select **View Certificate**.

   The Certificate window appears.
2. Select **Install Certificate**.

   The Certificate Import Wizard appears.
3. Click **Next**.

   The Certificate Store window appears.
4. Select **Automatically select the certificate store**, then click **Next**.

   The wizard complete panel appears.
5. Click **Finish**.

   The Root Certificate Store confirmation dialog box appears.
6. Click **Yes**.

   The Import successful dialog box appears.
7. Click **OK** twice.

   The Security Alert dialog box appears.
8. Click **Yes**.

   The Security Certificate installation is complete.

Creating a custom user catalog

The user’s authentication information (catalog and group) entered on the endpoint computer is passed to the Integrity Advanced Server when the user establishes a connection. The Integrity Advanced Server deploys and enforces policies based on the authentication data.

Create a user catalog named ‘test catalog’. For information about how to create a new user catalog, see the *Integrity Advanced Server Administrator Guide*.

Setting up the endpoint computer

Use the client packager to deploy Integrity Flex to an endpoint computer. For information about using the client packager, see the *Integrity Advanced Server Administrator Guide*. Do not deploy Integrity Agent in silent mode.

Performing the Integrity Advanced Server tests

This section explains how to verify that the Integrity client can establish a session, send heartbeats, and receive policy and configuration information from Integrity Advanced Server.

To perform the Integrity Advanced Server tests:

1. Create, deploy, and assign a new policy to the client.

   See "Create, deploy, and assign a new policy to the client," on page 84.

2. Verify the Integrity Server session.

   See "Verifying the Integrity Advanced Server session on the Integrity client," on page 87.

⚠ All the components in the Integrity Advanced Server system, including the database instances, RADIUS server, and Apache httpd server must be running to perform the steps in this section.

Create, deploy, and assign a new policy to the client

Assign a new policy to the client and verify that the client receives it.

To create, deploy, and assign a new policy to the Integrity client

1. Create and deploy a new policy.

   See "Creating and deploying a new policy, Test1," on page 85.

2. Assign the policy to the user catalog

   See "Assigning the Test1 policy to the user catalog," on page 86.

Creating and deploying a new policy, Test1

Create and deploy a test policy to verify that the client is checking for and receiving policies when they are assigned.

> For more information on creating and deploying policies, refer to the *Integrity Advanced Server Administrator Guide*.

To create and deploy the Test1 policy:

1. Log in to the Administrator Console using the masteradmin account.
2. Go to **Policies**.

   The Policy Manager page appears.
3. Click **New** and select **From Template**.

   The Create New Policy page appears.
4. Select the **Observation** policy template and type "**Test1**" in the Policy name text box.
5. Click **Create**.

   The Policy Settings page appears.
6. Click **Save**. This saves the policy with the preconfigured settings only.
7. Enter version comments and click **Save and Deploy**.
8. Click **Yes** to confirm deployment.

   The Policy Manager page appears with Test1 in the Policy list.

Assigning the Test1 policy to the user catalog

Assign the Test1 policy to your user catalog.

To assign the Test1 policy:

1. Log in to the Administrator Console.
2. Go to **Entities**.

   The Entity Manager page appears.
3. Select the catalog called ‘test catalog’ and click **Assign Policy**.

   The Assign Policies page appears.
4. In the Policy dropdown list, select **Test1**.
5. Click **Assign**.
6. Click **Yes** to confirm the assignment.

   The Entity Manager page appears, showing Test1 as the catalog’s assigned policy.

Verifying the Integrity Advanced Server session on the Integrity client

Once the policy is assigned, the Integrity client gets the Test1 policy after the next heartbeat.

> By default, Integrity Flex displays an Alert when it downloads a new policy. Integrity Agent does not display alerts of any type.

To check the client's policy:

1. On the endpoint computer, right-click the Integrity Flex icon in the system tray.

   The Control Window opens with the Test1 policy listed.

2. Go to the Policy tab.

   The Policy panel appears with the Test1 policy active.

The Test1 policy was downloaded and is now being used by the Integrity Flex client.

Chapter 6

Maintaining Integrity Advanced Server

Once you have installed and configured the Integrity Advanced Server you must periodically perform maintenance tasks to ensure optimum performance.

Monitor your database tablespace

Periodically check that you have sufficient free tablespace in your database. Databases can fill up quickly if you have:

- large numbers of client packages
- large numbers of users

Update your database statistics

When using Oracle 9*i* or Microsoft SQL Server 2000, you should periodically update your database statistics. Doing this will help your databases to work more efficiently, improving performance.

Optimize query performance

Some report queries may run for a long time, especially when filtering over a long time span. You should periodically run commands to optimize your query performance.

Optimizing query performance for Oracle 9i

Run the ANALYZE command on a regular basis to ensure optimal query performance. If you see the error '`ORA-01555: snapshot too old`' in the Integrity logs, increase the size or number of rollback segments.

Monitor your disk space

Closly monitor the Integrity Advanced Server disk space usage. Integrity and Apache logs can consume a lot of disk space on the Integrity Advanced Server. Integrity Advanced Server will fail to respond to Integrity clients and/or not work as expected if there are no free disk space. You should monitor the disk usage, and remove old logs as needed. Monitor the 'integrity/logs' directory on the Integrity Advanced Server.

Index