Editor's Notes: ©2006 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecurRemote, SecurServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, Zone Alarm Pro, Zone Labs, and the Zone Labs logo, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726 and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.
# Contents

Chapter 1:
Integrity Advanced Server Overview ................................................................. 1  
  Integrity Advanced Server system components ........................................ 2  
    System requirements ................................................................................. 2  
    Single host deployments ........................................................................... 2  
    Clustered Integrity Advanced Server ....................................................... 3  
  Integrity Advanced Server communications .............................................. 4  
    Integrity Advanced Server services and ports ....................................... 4  
    IAS services details .................................................................................. 6  

Chapter 2:
Installing and Configuring the Integrity Advanced Server ...................... 7  
  Clustering Integrity Advanced Servers ....................................................... 7  
  Backing up an existing installation ............................................................. 7  
  Upgrading and Migrating Integrity Advanced Server ............................... 8  
  Performing a New Integrity Advanced Server Installation ....................... 8  
  Configuring the databases and gathering information ............................ 9  
  Synchronizing Clocks ................................................................................ 12  
  Running the Installer .................................................................................. 13  
  Installation Information .............................................................................. 14  
    Installation types .................................................................................... 14  
    Server Type .......................................................................................... 14  
    Server Properties .................................................................................. 15  
    Domain Options ...................................................................................... 15  
    Clustering Options .................................................................................. 15  
    Clustering Information ............................................................................ 15  
    Database Information ............................................................................. 16  
    Setting Client Languages ....................................................................... 17  
    Completing the installation .................................................................... 18  
  Configuring the RADIUS Server ................................................................. 18  
    Prerequisites ........................................................................................... 18  
    Updating the configuration file ............................................................... 19  
    Configuring the properties file ............................................................... 19  
    Copying the files to the cluster ............................................................... 20  
  Configuring Integrity Advanced Server Cluster Load Balancer ................. 20  
    Setting up the virtual server ................................................................... 20  
    Setting status verification ....................................................................... 21  
  Using Integrity with a proxy server ............................................................ 22  
  Updating the logo ...................................................................................... 23
Chapter 3:
Starting and Stopping Integrity Advanced Server .................. 24
  Managing a Windows Setup ........................................ 25
  Stopping, starting, and resetting the services .................. 25
  Managing a Linux Setup ............................................ 26
  Starting, stopping, and restarting the Integrity Advanced
    Server ................................................................. 26
  Starting, stopping, and restarting the Apache server ...... 26

Chapter 4:
Migrating Data ................................................................. 27
  Understanding Data Migration ...................................... 27
  Migrated data ............................................................ 27
  Data that is not migrated ............................................ 28
  Migrating your Data .................................................... 28
  Running the Installer ................................................. 29
  Completing the Migration Pages ................................ 29
  Redeploy policies to users .......................................... 30

Chapter 5:
Setting Up System Event Logs ............................................. 31
  Understanding events and logging ................................. 32
    Recommended event logs ......................................... 33
  Using SNMP with Integrity ........................................ 36
    General Information ............................................... 36
    Trap Formats ....................................................... 36
  Managing events ....................................................... 37
    Creating and editing events ...................................... 37
    Deleting event ..................................................... 37
  Sending Logs to the SmartCenter Server ....................... 38
    Configuring SmartDashboard .................................. 38
    Configuring Integrity Advanced Server .................... 39
    Creating a Custom Query ....................................... 39

Chapter 6:
Testing Integrity Advanced Server ...................................... 40
  Setting up the Integrity Advanced Server test ............... 41
    Logging on to the Integrity Advanced Server Administrator
    Console ............................................................. 41
    Creating a custom user catalog ................................ 43
  Performing the Integrity Advanced Server Tests .......... 44
    Create, deploy, and assign a new policy to the client .... 44
    Verifying the Integrity Advanced Server session on the
      Integrity client ............................................... 47
Chapter 7: Maintaining Integrity Advanced Server ....................................... 48
  Monitor your database tablespace ............................................. 48
  Update your database statistics .............................................. 48
  Optimize query performance .................................................. 48
  Monitor your disk space ....................................................... 48

Index ....................................................................................................... 50
This chapter describes Integrity Advanced Server components and communications.

- “Integrity Advanced Server system components,” on page 2
- “Integrity Advanced Server communications,” on page 4
Integrity Advanced Server system components

This section provides an overview of the Integrity Advanced Server system components. Integrity Advanced Server is scalable and can be deployed on one host in smaller environments or clustered in a server farm on many hosts to support a high volume of connections in a larger environment.

System requirements

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

Single host deployments

Figure 1-1 shows the Integrity Advanced Server system installed on a single host and configured with the additional components required to operate the system. The Integrity Advanced Server system components are:

1. Integrity Advanced Server with a configured Apache httpd server
2. Integrity clients (Integrity Flex and/or Integrity Agent)
3. RADIUS server (optional)*
4. Database server*

Figure 1-1: Single Integrity Advanced Server host configuration
Clustered Integrity Advanced Server

Figure 1-2 shows the Integrity Advanced Server system cluster. In a distributed installation, Integrity Advanced Server is installed on several different hosts and configured with the additional components required to operate the system.

Use the instructions in Chapter 2, "Installing and Configuring the Integrity Advanced Server" to set up all Integrity Advanced Server nodes in a cluster. Differences between single and clustered configurations are noted.

The additional system components are:

- **Load balancer**: Routes traffic to/from Integrity Advanced Server.
- **NTP server (Optional)**: An internal or external server that ensures all Integrity Advanced Server hosts have the same time and date.

**Figure 1-2**: Clustered Integrity Advanced Server Configuration

* These components are not supplied as part of the Integrity Advanced Server distribution, and must be obtained from a third party. You may use a RADIUS server, or use the Integrity Advanced Server’s Administrator Authentication feature for authentication.
Integrity Advanced Server communications

This section explains the internal and external communication protocols and ports used by the Integrity Advanced Server and the Apache httpd server.

Integrity Advanced Server operations are implemented by separate Integrity services. An Apache httpd server proxies requests to these services from entities external to Integrity Advanced Server, such as Integrity clients or administrators logging on to Integrity Advanced Server from remote computers. The Apache httpd server acts as a single point of entry, managing requests using SSL, file caching, UDP, and/or TCP socket off loading functionality (see page 4).

This service and proxy configuration enables Integrity Advanced Server to be set up in a highly scalable and fault-tolerant clustered environment.

Integrity Advanced Server services and ports

The diagram below represents the services that make up Integrity Advanced Server and shows which ports the services use.

The services are divided into two types:

- **Client services** allow an Integrity client to get configuration information, policies, and communicate session state information.

- **Administration services** allow administrators to create groups and users; manage policies; manage system configuration; and perform other administrative tasks.

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

- 80
- 443
- 6054
Figure 1-3: Integrity Advanced Server services and ports
IAS services 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 httpd server configuration files. The URL is the service location information embedded in the request from the client that allows the Apache httpd server to proxy requests.

<table>
<thead>
<tr>
<th>Service name</th>
<th>Configuration name</th>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Manager</td>
<td>service.enable.connectionManager</td>
<td>/cm/*</td>
<td>Synchronizes 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. Also sends heartbeats to communicate policy or state changes.</td>
</tr>
<tr>
<td>Policy download</td>
<td>service.enable.policy</td>
<td>/policy/*</td>
<td>Policy download service.</td>
</tr>
<tr>
<td>Log upload</td>
<td>service.enable.logUpload</td>
<td>/logupload/*</td>
<td>Provides the mechanism endpoint computers use to upload client log files.</td>
</tr>
<tr>
<td>Program permission</td>
<td>service.enable.logUpload</td>
<td>/ask/*</td>
<td>Provides the mechanism endpoint computers use to upload client log files.</td>
</tr>
<tr>
<td>Sandbox server</td>
<td>service.enable.sandbox</td>
<td>/sandbox/*</td>
<td>Serves remediation Web pages to non-compliant, authenticated endpoint users.</td>
</tr>
<tr>
<td>Package Manager</td>
<td>service.enable.package</td>
<td>/package/*</td>
<td>Serves the client installer packages that install an Integrity client on an endpoint computer.</td>
</tr>
<tr>
<td>Administrator Console</td>
<td>service.enable.adminConsole</td>
<td>/</td>
<td>Serves the user interface that allows administrators to manage the Integrity Advanced Server.</td>
</tr>
</tbody>
</table>

Table 1-1: Description of Integrity Services
This chapter describes the configuration and installation steps you need to perform to get your Integrity Advanced Server system up and running. It contains the following topics:

- “Clustering Integrity Advanced Servers,” on page 7
- “Backing up an existing installation,” on page 7
- “Upgrading and Migrating Integrity Advanced Server,” on page 8
- “Performing a New Integrity Advanced Server Installation,” on page 8
- “Configuring the databases and gathering information,” on page 9
- “Synchronizing Clocks,” on page 12
- “Running the Installer,” on page 13
- “Installation Information,” on page 14
- “Configuring the RADIUS Server,” on page 18
- “Configuring Integrity Advanced Server Cluster Load Balancer,” on page 20
- “Using Integrity with a proxy server,” on page 22
- “Updating the logo,” on page 23

### Clustering Integrity Advanced Servers

When deploying a cluster of Integrity Advanced Servers, you should first configure and test a single Integrity Advanced Server. After you confirm that the single server is functioning properly, install and configure Integrity Advanced Server on the remaining nodes of the cluster. When deploying a clustered environment, make sure that all the node clocks are synchronized. Instructions specific to clustered environments are given where appropriate in this document.

### Backing up an existing installation

If you are upgrading from an existing Integrity installation, back up the current installation before you install the new version.
To back up your Integrity installation:

1. Make a copy of the entire home directory and save it to a safe location.
   
   The default is `C:\Program Files\Zone Labs\Integrity` for 5.x versions and `C:\Program Files\CheckPoint\Integrity` for 6.x versions.

2. Back up your database.
   
   If your installation includes an embedded database, your backup is already complete.
   
   If your installation uses a third-party database, use the preferred vendor-specific tool to back up the database.

Upgrading and Migrating Integrity Advanced Server

You can preserve some of the data from a previous installation of Integrity Advanced Server.

Before upgrading Integrity Advanced Server, you should first back up your existing installation. See “Back up an existing installation,” on page 7.

Integrity Advanced Server supports two methods of changing from an earlier to a later version of Integrity Advanced Server:

- **Upgrading** — To upgrade from 6.0.448.01 and later versions, select the Upgrade option in the installer. You will later be prompted to choose a location. Specify the current location of your Integrity installation.

- **Migrating** — To change to a higher version from an Integrity Advanced Server 5.x installation, you must install the new Integrity Advanced Server and migrate your data. See Chapter 4, Migrating Data, for more information. You can only migrate from versions that are 5.1 or later but prior to 6.0.

No other upgrades are supported.

Performing a New Integrity Advanced Server Installation

Use the steps in this chapter to perform a new Integrity Advanced Server installation.

**To install and configure the Integrity Advanced Server:**

1. Gather the database information and configure your databases.
   
   See “Configuring the databases and gathering information,” on page 9.

2. Synchronize clocks.
   
   See “Synchronizing Clocks,” on page 12.
3. Run the Integrity Installer.
   See “Running the Installer,” on page 13.

4. Configure the RADIUS server (optional).
   See “Configuring the RADIUS Server,” on page 18.

5. Configure load balancing (clustering only)
   See “Configuring Integrity Advanced Server Cluster Load Balancer,” on page 20

6. Customize the logo (optional).
   See “Updating the logo,” on page 23.

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:

<table>
<thead>
<tr>
<th>Database</th>
<th>Version</th>
<th>JDBC version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM DB2 ES 3.1</td>
<td>8.1.7</td>
<td>Bundled with the DB2 installation</td>
</tr>
<tr>
<td>Oracle</td>
<td>9.2.0.4.0</td>
<td>ojdbc14.zip (download from Oracle)</td>
</tr>
<tr>
<td>SQL Server</td>
<td>2000 SP3a</td>
<td>SQL Server Driver for JDBC SP3 (download from Microsoft)</td>
</tr>
<tr>
<td>J DataStore (Embedded)</td>
<td>7.2</td>
<td>Bundled with J DataStore</td>
</tr>
</tbody>
</table>

If you are using a single server, instead of a clustered system, you can choose to use the embedded database. 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.

If you are using a clustered environment, you will need to configure the maximum connections allowed by the database according to how many Integrity Advanced Servers you are using. By default, each Integrity Advanced Server uses a maximum of 150 JDBC connections at peak load, so you should configure your database to allow 150 * n connections, where ‘n’ is the number of Integrity Advanced Servers in your cluster.

To ensure good performance, you may have to periodically perform database maintenance. For more information about maintaining your database, see Chapter 7, “Maintaining Integrity Advanced Server,”.
To configure IBM DB2:

1. Create your database.
   Be sure to specify the UTF-8 character set.

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.

4. Create the Integrity Advanced Server database name.
   The preconfigured database name in Integrity Advanced Server is iss_main.

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

To configure Oracle 9i:

1. Create your database.
   Be sure to specify the UTF-8 character set.

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.

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.
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 names.
   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 with those on your database. If you are using clustering, you must synchronize all nodes on the cluster.

**To synchronize clocks in Linux:**

1. Use the `ntpd` 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.
Running the Installer

The Integrity Advanced Server installers use wizards to help you to install and configure your Integrity Advanced Server. There is a wizard for Windows installations and a wizard for Linux installations. Choose the installer appropriate for your system.

The Integrity Advanced Server Installer for Windows

To run the Integrity Advanced Server Installer for Windows

1. Double click the ISSetup_X_X_XXX_X.exe file.
   The Integrity Advanced Server Installer for Windows starts.

2. Follow the instructions in the wizard to complete your installation. See “Installation Information,” on page 14 for help in completing the wizard.

The Integrity Advanced Server Installer for Linux

To run the Integrity Advanced Server Installer for Linux

1. Log in as root.

   [root@localhost /]

2. Change the permissions on the ISSetup_X_X_XXX_X.bin file.

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

3. Run the ISSetup_X_X_XXX_X.bin.
   The Integrity Advanced Server Installer for Linux starts.

4. Follow the instructions in the wizard, entering the information for your installation.
   See “Installation Information,” on page 14 for help in completing the wizard.
   To go back to the previous step, type ‘back’.

The installers create the following directories:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache2/</td>
<td>Contains the pre-configured Integrity Apache server</td>
</tr>
<tr>
<td>apache2/conf</td>
<td>Apache configuration</td>
</tr>
<tr>
<td>apache2/conf/ssl</td>
<td>Apache ssl configuration and certificates</td>
</tr>
<tr>
<td>engine/</td>
<td>Contains Integrity Service</td>
</tr>
<tr>
<td>engine/jdk</td>
<td>The location of the Java JMI</td>
</tr>
</tbody>
</table>

Table 2-1:

By default the directories are created in /usr/local/checkpoint/integrity.
Installation Information

Use the following information to complete the installation wizards.

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.

    See Chapter 4, Migrating Data, for more information about upgrading from 5.x versions.

- **Upgrade from 6.x**—Use this option to upgrade from version 6.0.448.001 or later.

  Make sure you have backed up your system before choosing this option. See “Backing up an existing installation,” on page 7.

- **Join Cluster Installation**—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.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>engine/webapps/ROOT</td>
<td>The location of the Integrity Web application</td>
</tr>
<tr>
<td>engine/webapps/ROOT/bin</td>
<td>The location where some of the server utilities are hosted</td>
</tr>
<tr>
<td>logs/</td>
<td>All Apache, Tomcat, and Integrity logs. When monitoring a server, all log files in this directory should be monitored.</td>
</tr>
</tbody>
</table>

Table 2-1:

By default the directories are created in usr/local/checkpoint/integrity.
Server Properties

Enter the properties for your local server.

- **Local Host IP Address**—Enter the IP address or host name of the local server machine that the server will run on. If the machine has multiple NIC cards, then 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 that is used by the Integrity clients to connect to the server. In the case of a clustered installation, this 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 later install additional servers.

Clustering Information

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

- **Clustering Multicast Addresses**—These addresses 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 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.
- **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 16.
- **Database Name**—Enter the name of the database instance. See "Configuring the databases and gathering information," on page 9 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 IBM DB2 driver files**

You can obtain the IBM DB2 driver files from your DB2 host computer.

**To obtain the IBM DB2 drivers:**

1. Go to your DB2 host computer.
2. Copy the db2jcc.jar and db2jcc_license_cu.jar files to any location on the computer you wish to install Integrity Server on. Be sure to note the location.

**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. (In a clustered environment, shut down all Integrity nodes in the cluster.)
2. At the command line, go to `<install_dir>\engine\webapps\ROOT\bin`. (In a clustered environment, you can do this on any node in the cluster.)
3. 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. Integrity prompts you to change your password periodically. Passwords must be at least six characters long.

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.
- If you are migrating data from a 5.x version of Integrity Advanced Server, you should log into the Administrator console and complete the migration before making changes to the configuration file.

To configure the RADIUS server:

Perform the following steps to configure the RADIUS server. Configuration consists of updating a configuration file and a properties file. If you are using clustering, you will have to update these files on one computer and then transfer them to the other computers in the cluster.

1. Update the configuration file.
   
   See “Updating the configuration file,” on page 19.
2. Configure the properties file.
   See “Configuring the properties file,” on page 19.
3. Copy the files to the rest of the cluster. (Clustering)
   See “Copying the files to the cluster,” on page 20.

**Updating the configuration file**

To update the configuration file:
1. Shutdown the Integrity Advanced Servers.
2. Log in as root.
3. Go to \CheckPoint\Integrity\engine\webapps\ROOT\install\templates\config
   In Linux, the path is in lower case.
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 your changes and close the file.
   Make sure your XML is well-formed.

**Configuring the properties file**

To configure the properties file:
1. Go to CheckPoint\Integrity\engine\webapps\ROOT\install\templates.
   In Linux, the path is in lower case.
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 CheckPoint\Integrity\engine\webapps\ROOT\bin directory and run upgradeServer.bat (Windows) or upgradeServer.sh (Linux).

   If you are migrating from Integrity 5.x do not run these utilities until you have logged into the Integrity server to complete the migration.

7. Restart the Integrity Advanced Server.

**Copying the files to the cluster**

If you are using clustering, you must perform the steps above on one computer, then copy the configured files to the other computers in the cluster.

**To copy the files to the cluster**

1. Copy the template-integrity-config.xml and install-upgrade.properties files to the appropriate locations on the other Integrity Advanced Servers.

2. Restart the Integrity Advanced Servers.

**Configuring Integrity Advanced Server Cluster Load Balancer**

This section explains the minimum set up requirements for the cluster load balancer. The load balancer routes the traffic to two or more Integrity Advanced Server nodes.

**To configure load balancing:**

1. Set up the virtual server.
   
   See “Setting up the virtual server,” on page 20.

2. Configure status verification.
   
   See “Setting status verification,” on page 21.

**Setting up the virtual server**

For a simple installation, create a “Round Robin” virtual server with multicasting enabled and open the following ports to traffic:

- HTTP (TCP 80)
- HTTPS (TCP 443)
Setting status verification

Configure a load balancer service to check that each Integrity Advanced Server node is up and running. To check system status, set up an HTTPS get on URL: “https://{Integrity_IP}/systemstatus” (where {Integrity_IP} is the Integrity Advanced Server IP address). Compare the system status file from each Integrity Advanced Server node.

Set up the load balancer to direct traffic using the following state information reported in the system status file. Compare the file contents to the following messages and set up routing accordingly. When the returned text is:

- **System status: OK** It indicates that the node is functioning properly. Point traffic to the node.
- **System status: Error** It indicates that the node is not functioning properly. Do not point traffic to the node.

The administration services traffic requires persistence with at least 60 seconds of “stickiness”. Most session replication occurs in less than a second. However, setting the interval to 60 seconds ensures that the server has enough time to replicate data under a heavy load.

- ZSPHB (UDP 6054)
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,” in the Integrity Advanced Server Administrator Guide. For information on Anti-Spyware, see Chapter 11, “Policies: Protecting Against Spyware,” in the Integrity Advanced Server Administrator Guide.

Configuration steps are are provided for the following operating systems:

- “Windows,” on page 22
- “Linux,” on page 22

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 \Integrity\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 integrityd by issuing:

   `/etc/init.d/integrityd stop`
   `/etc/init.d/integrityd start`

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 specify the image file for your logo.

**To update the logo:**

1. Log in as root.

   `[root@localhost /] #`

2. Copy your logo image file over the default file.

   `[root@localhost /usr/local] # cp engine/webapps/ROOT/images/misc/<your_logo>.png engine/webapps/ROOT/images/misc/cobrand_logo.png`

The Integrity Advanced Server user interface will now display your logo.
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.

In order for the 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,” on page 25
  - “Stopping, starting, and resetting the services,” on page 25
- “Managing a Linux Setup,” on page 26
  - “Starting, stopping, and restarting the Integrity Advanced Server,” on page 26
  - “Starting, stopping, and restarting the Apache server,” on page 26
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

2. Right click on the service and choose the option you want.
Managing a Linux Setup

Starting, stopping, and restarting the Integrity Advanced Server

This section explains how to start, stop, or restart, the Integrity Advanced Server only.

To start, stop, or restart the Integrity Advanced Server only:

1. Log in to the Integrity Advanced Server host as root.
   [root@localhost ] #
2. Run the start, stop, or restart shell:
   - Start: /etc/init.d/integrityd start
   - Stop: /etc/init.d/integrityd stop
   - Restart: /etc/init.d/integrityd restart

   The Integrity Advanced Server starts, stops or restarts.

Starting, stopping, and restarting the Apache server

This section explains how to start, stop, or restart, the Apache httpd server only.

To start, stop, or restart the Apache httpd server only:

1. Log in to the Integrity Advanced Server host as root.
   [root@localhost ] #
2. Run the start, stop, or restart shell:
   - Start: /etc/init.d/httpd start
   - Stop: /etc/init.d/httpd stop
   - Restart: /etc/init.d/httpd restart

   The Apache httpd server starts, stops or restarts.
Chapter 4

Migrating Data

Use the steps in this chapter to migrate your data from Integrity Server versions 5.1 or later that are prior to 6.0. For information on upgrading from 6.x installations, see “Upgrading and Migrating Integrity Advanced Server,” on page 8.

Migration from single domain installations to a multi domain installation is not supported. Migration from one database type to another is not supported. Integrity Advanced Server version 6.0 and 5.x versions cannot run simultaneously on the same computer and you must create new database schemas for the new installation.

The best practice for upgrading is to install the new Integrity Advanced Server, perform the migration steps to transfer your data, then test the new server with a limited deployment. Once you have had a successful limited deployment you can deploy to your entire enterprise and shut down the old Integrity Advanced Server.

Understanding Data Migration

Data migration allows you to move some of your data from a previous installation of Integrity Server to your new installation. Any data that you did not create settings for will be set to the default values.

Note that migrating from 5.x version to 6.x versions and then upgrading to a later 6.x version may cause unexpected legacy data to appear. If you have previously migrated data to an earlier version of Integrity Advanced Server and then upgrade to the most recent version, data that you configured in the earliest (5.x) version may appear in the latest version, even if it did not appear in the intermediate version. This is due to differences in feature availability between versions.

Migrated data

The following data is migrated:

- Policies (most data)
- Policy items that are used in policies:
  - Firewall Rules
  - Protocols
  - Locations
  - Mail-Safe Extensions
  - Enforcement Rules.
  - Program/Group Permissions
- Observed programs
- Program groups and individual programs that are included in a policy
- Antivirus rules
- Reference sources
- IM Security settings

**Data that is not migrated**

The following data is not migrated:

- Certain portions of policies (client minimum version)
- Any program with invalid or missing checksums.
- Any program permissions in policies for dropped programs
- Catalogs
- Gateways
- Policy assignments
- Programs not included in a policy
- Disabled firewall rules
- Outbound MailSafe Settings
- Heartbeat and log transfer settings
- Gateway MAC addresses
- Sources and destinations in firewall rules
- Any data not explicitly mentioned above as being imported.

**Migrating your Data**

To migrate your data, perform the usual installation steps, selecting the appropriate migration options in the installer, and completing the migration pages in the Integrity Server Administrator Console.

**To install and migrate your data:**

1. Gather the database information and configure your databases.
   
   You must create new database schemas for the new installation. See “Configuring the databases and gathering information,” on page 9.

2. Synchronize clocks.
   
   See “Synchronizing Clocks,” on page 12.
3. Run the Integrity Server Installer, choosing the appropriate options.
   See “Running the Installer,” on page 29.

4. Log in and complete the migration pages in the Integrity Server Administrator Console.
   See “Completing the Migration Pages,” on page 29.

5. Customize the logo (optional).
   See “Updating the logo,” on page 23.

6. Redeploy policies to users
   See “Redeploy policies to users,” on page 30.

**Running the Installer**

To run the installer:

1. Start the installer.
   See “Running the Installer,” on page 13 for general information about running the installer.

2. Choose the **New Install** option.

3. Proceed through the installer, selecting your options as appropriate.
   Be sure to select the **Import data from existing Integrity System** option. For more information about running the installer see “Installing and Configuring the Integrity Advanced Server,” on page 7.

4. Click **Done**.

**Completing the Migration Pages**

To complete the migration pages:

1. Log into the Integrity Server Administrator Console with the default login name and password settings: masteradmin/password
   You will be prompted to change your password.

2. Change your password and click **OK**.
   The Integrity Migration page appears.

3. In the first migration page, enter your database type.

4. Complete the second migration page with your database information and click **Run Migration**.
   If you are using an embedded database and it is located on a different computer, copy the \.../Repository/data directory with all its content from that computer to
the current computer and select the database file integrity.jds. The fields you see on this screen vary according to which database type you choose. If your migration is successful, you will receive a report.

If you cancel the migration process, you will not have another opportunity to import your data. You will need to uninstall the Integrity Advanced Server then reinstall it to migrate your data.

**Redeploy policies to users**

Once you have successfully migrated your old data, you will need to redeploy your policies to users.

**To perform a phased redeployment:**

1. Decide on a set of users that will start using the new system, and what type of policy they might need.
2. Log into the new Integrity Advanced Server Administrator Console.
3. Create client packages.
4. Set Program Advisor license, (if applicable).
5. Create and import catalogs into the new system.
6. Set policy assignments for the pilot users.
7. Deploy packages to the pilot group of users.

The package should migrate the users to the new Integrity client.

Use the pilot period to test your policy settings and Program Advisor (if applicable). When the pilot period is over distribute packages to all users. When the old Integrity server indicate no current connections you may turn it off.
Chapter 5
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,” on page 32
- “Using SNMP with Integrity,” on page 36
- “Managing events,” on page 37
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.
- **JDBC** — 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 33
- "Routing Log Upload System warn and error messages to e-mail and pager accounts (SMTP)," on page 34
- "Adding warn, error, and fatal messages to a system log (syslog)," on page 35

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.

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

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

All nodes in the Integrity Advanced Server cluster append events to the same remote SYSLOG server when the syslog is stored somewhere other than an Integrity Advanced Server node. If you choose create a local syslog, each node creates a log and records only events which happen on that host.

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>System Log</td>
<td>Identifies the event to Integrity administrators.</td>
</tr>
<tr>
<td>Description</td>
<td>System status events.</td>
<td>Describes the event type to Integrity administrators.</td>
</tr>
<tr>
<td>Type</td>
<td>syslog</td>
<td>Causes Integrity to write events to a system log file.</td>
</tr>
<tr>
<td>Log Levels</td>
<td>Warn, Error, and Fatal</td>
<td>Specifies the types of events to log. It is recommended to log all these event types.</td>
</tr>
<tr>
<td>Event Classes</td>
<td>All</td>
<td>Specifies the types of events to log.</td>
</tr>
<tr>
<td>Server hostname</td>
<td>Host name or IP address of syslog server</td>
<td>Specifies the server Integrity will use to send messages. (For example, use 127.0.0.1 to store locally.)</td>
</tr>
<tr>
<td>Facility</td>
<td>USER</td>
<td>Enter the name of the syslog-facility handling Integrity Advanced Server event messages.</td>
</tr>
</tbody>
</table>
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 37.

Trap Formats

Traps include a header and a message. All traps have a common header, as they are all 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 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. Use the online help for specific event types, event class, and log level details.

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.
   Other nodes in the cluster implement the changes the next time the administration services are replicated to the node.

Deleting event

Deleting an event from Integrity Advanced Server completely removes it from the system. Integrity immediately stops recording and sending events from the local host.
In a clustered environment, other nodes in the cluster stop sending information the next time the administrative services are replicated.

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.
Once you have installed and configured the Integrity Advanced Server and started all the components, you are ready to set up the 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 the 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 41.

2. Perform the test.
   
   See “Performing the Integrity Advanced Server Tests,” on page 44.
Setting up the Integrity Advanced Server test

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

For detailed instructions on using the 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 41.

2. Create a user catalog.
   See “Creating a custom user catalog,” on page 43.

3. Set up the endpoint computer.
   See “Setting up the endpoint computer,” on page 43.

Logging on to the Integrity Advanced Server Administrator Console

The Integrity Advanced Server comes preconfigured with one administrator account, masteradmin.

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

This section explains how to verify that Integrity client can establish a session, send heartbeats, and receive policy and configuration information from the 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 44.

2. Verify the Integrity Server session.
   See “Verifying the Integrity Advanced Server session on the Integrity client,” on page 47.

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 45.

2. Assign the policy to the user catalog
   See “Assigning the Test1 policy to the user catalog,” on page 46.
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 Administration Console using the masteradmin account.
2. Select the domain to which the user is assigned.
3. Go to Policies.
   The Policy Manager page appears.
4. Click New and select From Template.
   The Create New Policy page appears.
5. Select the Observation policy template and type “Test1” in the Policy name text box.
6. Click Create.
   The Policy Settings page appears.
7. Click Save. This saves the policy with the preconfigured settings only.
8. Enter version comments, click Save and Deploy.
9. 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 Administration Console and select the domain.
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.
   The Confirm Policy Assignment page appears.
6. Click Assign.
   The Assign Policy page appears with the “Deployed Policy” of the catalog as Test1.
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 7

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 9i, IBM DB2 8.2, 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 DB2

Run the DB2 RUNSTATS command on the reporting tables and indexes on a regular basis. In some circumstances, queries may time out and errors will appear in the logs. If this occurs increase the amount of time for TCP/IP timeouts to keep connections alive longer.

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

Closely 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.
A
administration services 4
Apache HTTP server
   in single-host deployment 2
   starting and stopping 26
C
client services 4
clustered system deployment 3
D
DB2 database
   configuring 9
   in single-host deployments 2
I
Integrity Advanced Server
   clustered system deployment 3
   installing 7–18
   load balancer, configuring 20
   services and ports 4
   single-host deployment 2
   starting and stopping 24–26
   system components 2
   verifying status of 21
Integrity clients 2
Integrity services, described 6
L
load balancer, configuring 20
P
Program permission 6
R
RADIUS server
   in single-host deployments 2
Root Certificate Store, confirming 42
S
single-host deployments 2
system status, verifying 21