# Administrator Guide

Using Integrity Advanced Server

Check Point SOFTWARE TECHNOLOGIES LTD. integrity

1-0282-0650-2006-04-07

# Contents

# Chapter 1
# Introduction

This chapter provides an overview of the Integrity Advanced Server Administrator Guide and of the Integrity Advanced Server documentation.

# About this Guide

This Administrator Guide is intended for administrators responsible for day-to-day security management tasks within an enterprise, including policy management and user support.

For information on installing and configuring Integrity Advanced Server at the system level, and on monitoring system health, see the Integrity Advanced Server Installation Guide.

This guide contains the following chapters with information needed by enterprise administrators.

# Document Overview

| | Title | Description |
|---|---|---|
| 2 | Configuring and Managing Catalogs and Groups | ■ How to add user catalogs and groups |
| 3 | Managing Administrators | ■ Overview of role-based administration, privileges, and permissions<br>■ How to configure administrator accounts<br>■ How to assign roles, use default roles, and create customized roles for administrators |
| 4 | Managing Policies | ■ Overview of enterprise policies and personal policies<br>■ Rule evaluation and precedence<br>■ Tips for creating effective policies<br>■ A model policy life cycle |
| 5 | Policies: Classic Firewall Rules | ■ Overview of classic firewall rules<br>■ Creating re-usable port and protocol definitions and source and destination locations for use in firewall rules<br>■ Creating re-usable firewall rules<br>■ Adding firewall rules to a policy |
| 6 | Policies: Zone-Based Security | ■ Overview of Zones and Zone rules<br>■ Adding computers and networks to Trusted and Blocked Zones<br>■ Setting/modifying security levels applied to each Zone |
| 7 | Policies: Program Control | ■ “Observing” programs on your network<br>■ Creating and using reference sources<br>■ Creating and managing program groups<br>■ Creating program rules |
| 8 | Policies: Restricting Non-Secure Endpoints | ■ Overview of enforcement rules<br>■ What the user experiences when restricted<br>■ Minimizing user support impact of enforcement rules<br>■ Creating re-usable enforcement rules<br>■ Adding enforcement rules to policies |

**Table 1-1:** Chapters in this guide

| | Title | Description |
|---|---|---|
| 10 | Policies: Protecting Against Spyware | ■ Anti-Spyware overview<br>■ Configuring Anti-Spyware protection<br>■ Monitoring Anti-Spyware protection |
| 11 | Policies: Preventing E-mail Attacks | ■ How MailSafe works<br>■ Managing extensions (attachment type definitions) |
| 12 | Policies: Protecting Instant Messaging | ■ IM Security overview<br>■ Configuring IM Security<br>■ Monitoring IM Security |
| 13 | Gateways and Cooperative Enforcement | ■ How to configure gateways<br>■ How to setup cooperative enforcement |
| 14 | Delivering Policies and Policy Packages to Clients | ■ Assigning and deploying policies<br>■ Policy inheritance; direct and indirect assignments<br>■ Managing versions and rolling back to a previous version. |
| 15 | Integrity Client Installation Packages | ■ How to create and configure an Integrity client package |
| 16 | Monitoring Client Security | ■ Setting log upload parameters<br>■ Getting an overview of your endpoints<br>■ Finding details information about individual endpoints<br>■ Tracking enforcement-rule compliance<br>■ Tracking client security events<br>■ Monitoring programs on your network |

**Table 1-1:** Chapters in this guide

# Other Integrity Advanced Server Documentation

| Title | Description |
|---|---|
| Integrity Advanced Server Installation Guide | Contains detailed instructions for installing, configuring, and maintaining Integrity Advanced Server. |

**Table 1-2:** Integrity Advanced Server Documentation

| Title | Description |
|---|---|
| Integrity Advanced Server Administrator Console Reference | Contains screen-by-screen descriptions of user interface elements, with cross-references to relevant chapters of the Administrator Guide. This document contains an overview of Administrator Console navigation, including use of the help system. |
| Integrity Advanced Server Administrator Guide | Contains information on managing administrators and endpoint security with Integrity Advanced Server. |
| Integrity Advanced Server Gateway Integration Guide | Contains information on integrating your Virtual Private Network gateway device with Integrity Advanced Server. Also contains information regarding deploying the unified SecureClient/ Integrity client package. |
| Integrity Advanced Server System Requirements | Contains information on client and server requirements. |
| Integrity Agent for Linux Installation and Configuration Guide | Contains information on how to install and configure Integrity Agent for Linux. |
| Integrity XML Policy Reference Guide | Contains detailed information on the contents of Integrity client XML policy files. |
| 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. |

**Table 1-2:** Integrity Advanced Server Documentation

# Chapter 2
# Configuring and Managing Catalogs and Groups

This chapter provides instructions for setting up catalogs and groups, and assigning an Administrator to a catalog or group.

These instructions are intended primarily for administrators responsible for setup and maintenance.

# Entities and inheritance

Each enterprise can contain any number of user catalogs. Each user catalog in turn can contain any number of user groups. Catalogs and groups are referred to collectively as **entities**.

By default, entities inherit security policies and administrators from their parent entities.

## How administrator inheritance works

Any number of administrators can be assigned to an entity at any given time. Therefore assigning an administrator to an entity does not override another administrator's entity assignments.

Assigning an administrator to a:

- **User Catalog** gives the administrator access to that user catalog and all the user groups in that user catalog
- **User Group** gives the administrator access to only the user group

The following diagram illustrates the entity inheritance structure for an administrator.

.

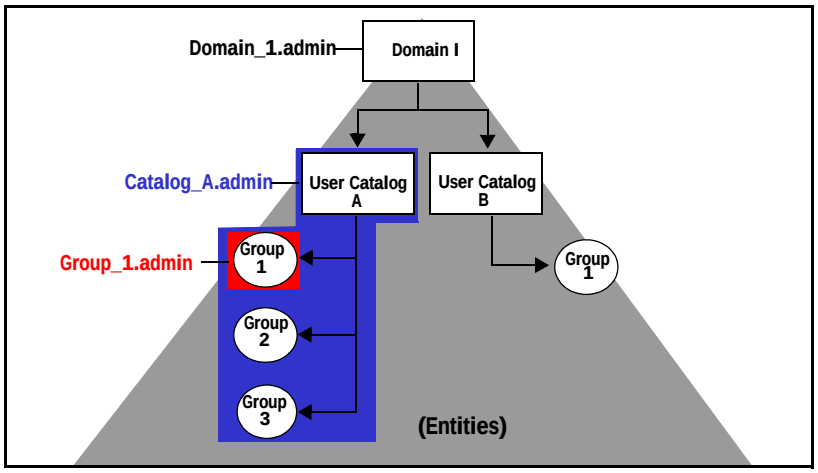



**Figure 2-1:** Administrator inheritance

### Example: Inheriting administrators

In Figure 2-1:

- Domain_1.admin is assigned to Domain 1. This administrator can access all the entities in Domain 1 (User Catalog A, User Catalog B, and every group).
- Catalog_A.admin is assigned to User Catalog A. This administrator can access User Catalog A and Groups 1-3 of User Catalog A.
- Group_1.admin is assigned to Group 1 of User Catalog A. This administrator can access only Group 1 of User Catalog A only.

# How policy inheritance works

You can assign only one policy to an entity at a time. When you assign a specific policy to an entity, the children of that entity inherit the policy. Assigning a policy to an entity overrides inheritance from the parent.

The diagram below illustrates the entity inheritance structure for policies.

.

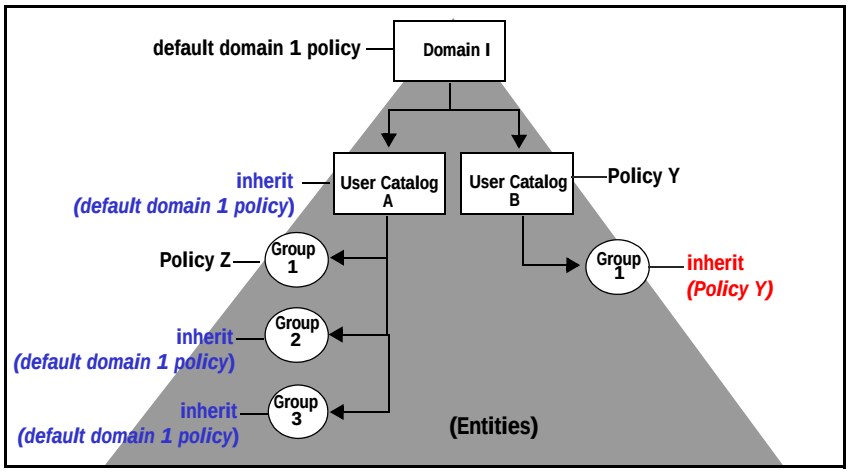



**Figure 2-2:** Policy inheritance

# Adding entities to the enterprise

Each enterprise in Integrity Advanced Server can contain any number of user catalogs. Each user catalog, in turn, can contain any number of user groups. Collectively, catalogs and groups are called “entities.”

By partitioning your enterprise into entities, you can assign different policies and administrators to different groups of users. (A user is a single user of an endpoint computer on which an Integrity client is installed, and whose identification is registered with Integrity Advanced Server.) Entities can be defined by IP address range, VPN gateway, user directory, or custom specifications.

Integrity Advanced Server identifies endpoints by their authentication information. Each catalog on Integrity Advanced Server must be unique. Catalogs cannot have the same name.

Before you assign an administrator or policy to an entity, you must create the entities that represent your enterprise.

When you configure user catalogs and groups, the name of the catalog or group must match the authentication server catalog or group name exactly.

## Using Entities: An Example

This section provides an example of how to use entities to assign different policies based on IP address ranges within a network. The example focuses on IP catalogs (catalogs based on IP addresses), but the steps outlined here can apply to custom catalogs and gateway catalogs as well.

Consider a desktop publishing company that uses many printers. The company wants to assign different policies to different host IPs in one of its divisions—one policy for endpoint desktops, the other for printers. To do this, an administrator would:

1. Create an IP catalog with the desired IP address range (for example, 172.00.00.00 to 172.00.00.250). (For details on creating IP catalogs, see “Adding an IP catalog,” on page 12.)
2. Assign a desktop-specific policy to the catalog. (For details, see “Assigning a policy to entities,” on page 162.)
3. Create an IP group for printers under the new IP catalog. The group would consist of comma-delimited printer IP addresses or hostnames (for example, 172.00.00.47, 172.00.00.63, and so on). (For details on creating groups, see “Adding groups to custom, IP, and gateway catalogs,” on page 17.)
4. Assign a printer-specific policy to the printer group.

Printers and endpoint computers would then be protected by two different policies, thus isolating printers from desktop policies.

# Authenticating users

Integrity Advanced Server can import user directory information from LDAP, NT Domain, and RADIUS servers, allowing users to be authenticated against those directories. Integrity uses NT Domain or certain LDAP directories (listed below) as native authentication systems, meaning that Integrity automatically recognizes users authenticated through those directories. If your organization uses another authentication system, such as RADIUS, you can configure Integrity to use it for proxy login. With proxy login, Integrity prompts users to log in for authentication.

Integrity Advanced Server performs authentication as follows:

- **Native authentication for NT Domain, Microsoft Active Directory, and Novell NDS LDAP.** If a user is authenticated via NT Domain, Novell NDS, or Microsoft Active Directory, Integrity automatically recognizes that user.
- **Proxy login for NT Domain, RADIUS, and LDAP directory users.** If your authentication system is RADIUS or LDAP (other than Novell NDS and Microsoft Active Directory), use proxy login. (To configure proxy login, select the **Proxy Login Server** checkbox when adding the relevant catalog.)

  With proxy login, Integrity does the following when an endpoint connects to the enterprise network:

  **a.** Displays a proxy login window and requires the user to authenticate.

  **b.** Authenticates the user-supplied user ID and password against the external user directory (NT Domain, RADIUS, or LDAP) and, if successful, assigns the appropriate security policy.

You can designate only one catalog (NT Domain, RADIUS, or LDAP) for proxy login.

- **Cooperative Enforcement for users who connect to the enterprise network through an Integrity-supported gateway** and do not already exist in an associated group. Users added in this way are placed in gateway catalogs.

## Proxy Login and Auto Add

Integrity Advanced Server's Auto Add feature adds users who are authenticated by proxy login to the user directory. If the Auto Add option is selected during the user directory import process, users will be placed in the appropriate group if they ever need to access the network via proxy login. Users must be authenticated on the LAN before they are auto-added. When Integrity Advanced Server auto-adds a user, it deploys the most recent policy to the endpoint.

Before you assign an administrator or policy to an entity, you must create the entities that represent your enterprise.

When you configure user catalogs and groups, the name of the catalog or group must match the authentication server catalog or group name exactly.

# Adding a custom catalog

Use the Administrator Console to add a custom catalog to the Integrity Advanced Server.

### To add a new custom catalog:

1. Go to **Entities**.
2. Click **New Entity** and select **Custom**.
3. Complete the catalog information:
   a. In the **Catalog Name** box, type the name of the catalog.
      The catalog name is not case-sensitive and is limited to 128 characters.
   b. In the **Catalog Description** box, type a description of the catalog.
      The description appears on the View and Edit pages only and is limited to 250 characters.
4. Click **Save**.

   The catalog is added.

After you have added a catalog, you can add groups to it. See "Adding groups to custom, IP, and gateway catalogs," on page 17.

# Adding a gateway catalog

Use the Administrator Console to add a gateway catalog to Integrity Advanced Server. Integrity works with supported gateways using the Cooperative Enforcement feature to provide endpoint security for remote endpoint computers. The first time a new user connects to Integrity Advanced Server, they are dynamically added to the gateway catalog or group.

### To add a new gateway catalog:

1. Go to **Entities**.
2. Click **New Entity** and select **Gateway**.
3. In the **Catalog SubTypes** field, choose your gateway type.
4. Complete the fields with the appropriate information for your gateway.

   For explanations of the fields, see the online help. For more information see "Gateways and Cooperative Enforcement," on page 155 and the *Integrity Advanced Server Gateway Integration Guide*.
5. Click **Save**.

   The catalog is added.

After you have added a catalog, you can add groups to it. See “Adding groups to custom, IP, and gateway catalogs,” on page 17. You cannot add a group to a Check Point InterSpect Gateway catalog.

# Adding an IP catalog

Use the Administrator Console to add an IP catalog to Integrity Advanced Server. You can assign a policy based on an IP address range rather than on endpoint users.

**To add a new IP catalog:**

1. Go to **Entities**.
2. Click **New Entity** and select **IP Catalog**.
3. Complete the catalog information:
   a. In the **IP Catalog Name** box, type the name of the catalog.
      The catalog name is limited to 128 characters and it is *not* case-sensitive.
   b. In the **Address Range** boxes, type the IP address range for this catalog.
   c. In the **Subnet Mask** boxes, type the subnet for this catalog, if any.
4. Click **Save**.

   The catalog is added.

After you have added a catalog, you can add groups to it. See “Adding groups to custom, IP, and gateway catalogs,” on page 17. To see an example showing how IP catalogs and groups can be used together, see “Using Entities: An Example,” on page 9.

# Adding a user directory catalog

Use the Administrator Console to add an LDAP, NT Domain, or RADIUS catalog to Integrity Advanced Server. Later, you can synchronize a catalog to the user directory to obtain updates.

For RADIUS directories no child groups are possible. All users are placed in a group with the name of the directory server.

For LDAP or NT Domain directories, you can import all users in a directory to a single catalog, or import only specific directory groups to a catalog.

## Adding an LDAP catalog

RFC 1777-compliant LDAP (Lightweight Directory Access Protocol) servers versions 2 and 3 are supported. Integrity provides the configuration filters for Novell eDirectory for Windows, Netscape Directory Server for Windows 2000, and Windows Active Directory Service (native/mixed mode). If you are using any other LDAP server, you must have the user and group filter information to import the directories to Integrity’s

database. You can generally find this information in the LDAP provider's documentation.

### To add a new LDAP catalog:

1. Go to **Entities**.
2. Click **New Entity** and choose **LDAP**.
3. In the **Catalog Subtypes** field, choose your LDAP type: **Custom**, **Microsoft ActiveDirectory**, **Novell eDirectory**, or **Netscape iPlanet**.

   To use an LDAP directory that is not one of the built-in types, choose **Custom** and enter the appropriate User Filter and Group Filter values. Any server that conforms to the LDAP 2.0 specification or greater can be imported using the Custom catalog subtype. Details for filtering syntax are generally available in the documentation for that LDAP provider.
4. Complete the fields with the appropriate information for your LDAP user directory, including proxy login and auto add selections.
5. Click **Import Groups** to display a list of LDAP groups to import.

   To import the LDAP groups, select a group in the left panel and use the right arrow button to move the LDAP user groups to the right panel. Set the order or priority of the groups you are adding by using the up and down buttons.
6. Click **Save**.

   The catalog is added.

When you finish, proceed to "Adding administrators," on page 23, to assign an administrator to the catalog.

### Troubleshooting LDAP Import Problems

LDAP directory servers can impose a limit on the size of results that are allowed to be returned from a query. The Active Directory LDAP implementation has a default limit of 1000 users. Currently, importing an LDAP directory with more users than the imposed limit will cause the user directory import to fail. The workaround is to raise the limit.

### To increase the size limit on query results:

1. Run `ntdsutil.exe` (located in `WINNT\SYSTEM32`)
2. At the prompt type "LDAP policies".
3. At the "ldap policy:" prompt type "connection".
4. At the "server connections:" prompt type "connect to server [servername]", where [servername] is the name of the LDAP server.

   You will be granted access (or not) using the credentials of the locally logged in user.

5. Type “q” to go back up a menu.
6. At the “ldap policy:” menu type “show values” to see the policy settings.
7. You can set any of these by typing “set [attribute] to [value]”. For example, the one we want is “MaxPageSize” so you would type “set MaxPageSize to 5000" to allow 5000 users to be imported at once.
8. Type “show values” again to confirm your changes.

   Pending changes are shown in parentheses.
9. When finished, type “commit changes”.

## Adding an NT Domain catalog

Integrity Advanced Server communicates with Domain Controllers via the NetBIOS protocol using TCP ports 137-139. In order for Integrity Advanced Server to import catalogs from an NT or Active Directory domain, you must have a WINS server with NetBIOS over TCP/IP enabled. On a Windows 2000 Server platform running Integrity Advanced Server, this setting can be confirmed through the following steps.

### To confirm server settings:

1. Right-click on **Network Neighborhood**.
2. Select **Properties**.
3. Right-click on **Local Area Connection**.
4. Select **Properties**.
5. Select **Internet Protocol (TCP/IP)**.
6. Select **Properties**.
7. Select **Advanced**.
8. Select the **WINS** tab.
9. Make sure the **Enable NetBIOS over TCP/IP** radio button is selected.
10. Click **OK**.

When Integrity Server and a Domain controller communicate, only user IDs are transferred. No passwords are transmitted.

### Active Directory Compatibility

Integrity supports Active Directory in native and mixed mode.

If you are using Windows NT Server 4.0 (SP6a) for your Primary Domain Controller or Backup Domain Controller, then you will need to install Microsoft’s ADSI (Active Directory™ Service Interfaces) libraries on those machines in order for Integrity Advanced Server to be able to import and synchronize domains. The ADSI extensions can be downloaded from the Microsoft site at http://www.microsoft.com/ntworkstation/

downloads/Other/adclient.asp. Please follow Microsoft's documentation for full details on installing and configuring the ADSI libraries on your Integrity Advanced Server.

### Considerations Before Importing NT Domains

The NT Domain import process into Integrity Advanced Server offers options to import all NT Domain users into one group or selecting individual NT groups to import. To import all NT Domain users into one group requires the Integrity service to be configured to run under an NT Domain account with logon as a service privilege.

### To change the Integrity Advanced Server's login credentials:

1. Open the Services tool via Administrative Tools/Services.
2. Highlight the Integrity service, right-click and select **Properties**.
3. Open the **Log On** tab.
4. The default for the "Log on as" credential will be the Local System Account. Click the **This account** radio button.
5. Click the **Browse...** button. This will open the Local Users and Groups for the Windows Server installation on the host.
6. From the Integrity service properties/**Log On** window, click **OK** after entering the appropriate credentials and passwords for your domain(s)

### To add a new NT Domain catalog:

1. Go to **Entities**.
2. Click **New Entity** and select **NTDomain**.
3. In the **Catalog SubTypes** field, choose how you want to structure your NT Domain catalog; **Import all users into one group** or **Select groups to import**.

- If you choose **Import all users into one group**, then the whole NT Domain that you entered in the **Domain Name** field will be imported into the new catalog.
  a. Complete the fields with the appropriate information for your NT Domain user directory, including proxy login and auto add selections.
- If you choose **Select groups to import**, then the **Import Groups** button displays.
  a. Complete the fields with the appropriate information for your NT Domain user directory, including proxy login and auto add selections.
  b. Click **Import Groups** to display a list of NT Domain groups to import.
  c. To import the NT Domain groups, select a group in the left panel and use the right arrow button to move the NT Domain user groups to the right panel. Set the order or priority of the groups you are adding by using the up and down buttons.

     Although a user can exist in more that one group within NT Domain, the user cannot exist in more that one Integrity Advanced Server group. Therefore, Integrity Advanced Server establishes an order of priority when it imports

specific groups from NT Domains. If a user exists in more than one NT Group, Integrity Advanced Server places the user only in the higher-priority group. If the user name is present in no NT Groups, then it will be added to the top level domain group when imported.

4. Click **Save**.

   The catalog is added.

When you finish proceed to "Adding administrators," on page 23 to assign an administrator to the catalog.

## Adding a RADIUS catalog

Integrity Advanced Server enables the importing of RADIUS users which can then be assigned appropriate policies at the user level. If you are going to assign policies only at the RADIUS directory level and not at the individual user level, then you do not need to import the RADIUS catalogs. Integrity Advanced Server adds users to its database when they are successfully authenticated during proxy login, and it assigns the RADIUS catalog-level policy automatically if you check the "Auto Add" box. Integrity Advanced Server supports all RFC 2865-compliant RADIUS software.

To import RADIUS catalogs into Integrity Advanced Server, your RADIUS users file needs to be copied to Integrity Advanced Server. This user data file should be formatted and placed in a convenient location. The encoding type of your RADIUS catalog should be ASCII format.

### To format a user data file:

1. Open the RADIUS catalog you exported from your RADIUS server in MS Notepad.

   Save the file as ASCII by selecting the appropriate format from the encoding drop-down menu. This saved file will be your user data file.

2. Open the user data file and note the string, beginning with the first column, contains user IDs. The only requirement for the user data file is that each username be terminated with a carriage return, a space, or a comma. Thus, a user ID starts each line and ends with a minimum of 1 space character. Integrity Advanced Server does not recognize any "comment" characters.

   Since the first column is the only one that needs proper formatting, the rest is not utilized by Integrity Advanced Server.

3. Move your user data file from your RADIUS server to Integrity Advanced Server. Use FTP, diskette, or another preferred method for this task since the user data file will need to be imported into Integrity Advanced Server in the next section.

### To add a new RADIUS catalog:

If you want to add a new RADIUS catalog and your RADIUS server is on the same computer as Integrity Advanced Server, log in to Integrity using the IP address rather than "localhost." To do this, open a browser and use the IP address (instead of the string "localhost") to access the Integrity Advanced Server login page; then log in as usual.

1. Go to **Entities**.
2. Click **New Entity** and choose **RADIUS**.

You must first export your RADIUS users to a text file. In the **User Data File** field, type the location and name of the text file that contains the exported RADIUS users.

3. Complete the fields with the appropriate information for your RADIUS user directory.

In the **Shared Secret** field, use the password for the Password Authentication Protocol (PAP) shared secret account.

4. Click **Save**.

   The catalog is added.

If you are clustering Integrity Advanced Servers, then you need to store RADIUS catalogs locally on each server.

When you finish proceed to "Adding administrators," on page 23 to assign an administrator to the catalog or group.

## Adding groups to custom, IP, and gateway catalogs

You can add user groups to custom, IP, and gateway catalogs (except for Check Point InterSpect Gateway catalogs). Adding groups allows you to assign different policies and administrators to subsets of users within a catalog. If every user in a catalog is going to receive the same policy or be managed by the same administrators, you may not want to add groups at this time. (To see an example showing how catalogs and groups can be used together, see "Using Entities: An Example," on page 9.)

### To add a user group:

1. Go to **Entities**.

2. Click on entity links or use the Search function to find the appropriate catalog. When the relevant catalog is in the Current Entity area of the page, click **New Group**.

   The New Group page appears.

3. In the **Group Name** box, type a name for the group. Note that every group in a catalog must have a unique name, though user groups in different catalogs can have the same name.

If you are naming a user group for a *gateway* catalog, observe the following rules (noting that all names are case-sensitive):

- For Check Point Firewall-1 and VPN-1 SecureClient, the group name must be "checkpoint".
- For the Cisco VPN 3000 Series concentrator, the group name must match the name defined on the concentrator.
- For the Nortel Contivity VPN switch, the group name must be "nortel".

4. If you are creating an IP group, type the relevant IP addresses or hostnames (delimited by commas) in the **Hosts** field. IP addresses in the group must fall within the IP address range of the respective catalog. (Note that, to resolve hostnames, Integrity Advanced Server must have access to a DNS server.)
5. Click **Save**.

When you finish, proceed to "Adding administrators," on page 23 to assign an administrator to the catalog or group.

# Renaming and removing entities

This section explains the impact of removing entities from Integrity Advanced Server, and provides step-by-steps instructions on how to do it.

## Deleting a user catalog

Deleting a user catalog removes the catalog and all its groups. Policies assigned to the deleted catalogs are still available in Policy Manager.

Deleted users are removed from Integrity Advanced Server, but the client software and policy at the user's computer remain functional. The personal policy will continue to be enforced, as will the enterprise policy, if it was configured to be enforced when the user is disconnected from Integrity Advanced Server. Authenticated users in directories that have been deleted are also cached in Integrity Advanced Server's memory, and the Policy Studio Assignments panel will continue to list those users until the server is restarted.

### To delete a user catalog:

1. Go to **Entities**.
2. Click on entity links or use the Search function to find to the appropriate entity.
3. When the relevant catalog appears in the Current Entity area of the page, click the  icon.

   A confirmation dialog listing the user catalog prompts you to verify your action.
4. Click **Yes**.

   The catalog and all its groups are removed from Integrity Advanced Server.

Users in a deleted catalog can no longer log on. If a user is logged on when their catalog is removed, the user session is restricted or terminated on the next heartbeat. The administrators assigned to the catalog or a group within the catalog are automatically logged off.

# Deleting a user group

Removing a group from the system automatically re-associates endpoint users with the parent catalog only. When you remove a group, Integrity Advanced Server automatically re-assigns the parent catalog's policy to the users in the group. All endpoint users that belonged to the group may still access the system. If an endpoint user is logged on when the group is removed, they receive the parent catalog policy at the next heartbeat.

### To remove a user group:

1. Go to **Entities**.
2. Click on entity links or use the Search function to find to the appropriate group.
3. When the relevant group appears in the Current Entity area of the page, click the  icon.

   A confirmation dialog listing the user group prompts you to verify your action.
4. Click **Yes**.

   The group is removed from Integrity Advanced Server.

# Synchronizing User Catalogs

Synchronizing brings Integrity Advanced Server's user catalogs and groups up-to-date with the data on your LDAP or NT Domain user directory servers.

When you synchronize, the following occurs:

- New records are added to Integrity. New users get their parent group policy. New groups get the default policy until a specific group policy is assigned.
- User or group records that no longer exist in the external user directory are removed from Integrity Advanced Server. Deleted users are not known to Integrity Advanced Server, but the agent software and policy at the user's computer remains intact. The "personal policy" will continue to be enforced, as will the enterprise policy, if it was configured to be enforced when the user is disconnected from Integrity Advanced Server.
- Groups that are renamed are treated as a deletion and re-addition of the group. In this case, policy assignments are lost, and must be reassigned under the new name.
- Unchanged records are left as they are. Assigned policies remain in force.

## Updating RADIUS catalogs

To update the user data information in a RADIUS catalog, you need to replace the user data file with an updated user data file. See "To format a user data file:," on page 16 for how to export and format an updated user data file.

If the user data filename and its location remain the same, then Integrity Advanced Server will automatically update the RADIUS catalog. However, if you change the filename or its location, then you need to update the RADIUS catalog using the **Edit RADIUS Catalog** page. Use this page also to update any other RADIUS catalog settings.

If you have clustered Integrity Advanced Servers, then you need to update the local RADIUS catalog on each server.

### To edit a RADIUS catalog:

If you are using a RADIUS server on the same machine as Integrity Advanced Server, in order to add a new RADIUS catalog, make sure to login to Integrity Server using the IP address rather than "localhost."

1. Go to **Entities**.

2. Click on entity links or use the Search function to find to the appropriate RADIUS catalog.
3. When the catalog appears in the Current Entity area of the page, click the  icon.
4. Complete the fields with the appropriate information for your RADIUS user directory.
5. In the **User Data File** field, update the name and location for the user data file, if it has changed.
6. Click **Save**.

# Scheduling Synchronization

You can set Integrity Advanced Server to automatically synchronize all synchronizable catalogs on a daily or weekly basis.

### To set an automatic synchronization schedule:

1. Go to **Entities**.
2. Using the **Synchronize** drop-down lists, choose the desired frequency (manual, daily, or day of the week) and time of day.
3. Click **Update**.

# Manual Synchronization

Use the Entity Manager to manually synchronize an entity.

### To manually synchronize an entity:

1. Go to **Entities**.
2. Click on entity links or use the Search function to find the appropriate catalog.

   When the catalog appears in the Current Entity area of the page, click the  icon.

# Adding administrators

After setting up entities, the next configuration step is to create an administrator account for the person who will be responsible for managing the catalog or group. The administrator account created in this section has permission to perform the following tasks:

- Manage administrator accounts
  - Add and remove administrator accounts
  - Create and assign roles
  - Assign administrator to entities
- Manage policies
  - Create and delete items in the Data Managers
  - Create, assign, and delete enterprise security policies
  - Roll back to previous versions of policies
- Run reports

### To add a administrator account:

1. Go to **System Configuration** | **Administrators**.

   The Administrator Manager page appears.

2. Click **New**.

3. Complete the administrator information:

   a. In the **Administrator ID** box, type the log on ID for the Administrator.

If the Integrity Advanced Server administrators are authenticated against an external database, the administrator ID must match the user name in the external database.

   b. In the **Title** box, type the title of the administrator.

   c. In the **Real Name** box, type the administrator's first and last name.

   d. In the **E-mail** box, type the e-mail address of the administrator.

4. Assign the **Account Administrator** role.

   a. In the **Assigned Role** list, click **Edit**.

   The Assign Role page appears.

   b. Select the **Account Administrator** role, click **Save**.

   The administrator role appears in the administrator's current role list.

The Account Administrator role allows access to all features and functions in the menu area.

**5.** On the **New Administrator** page, click **Save**.

# Chapter 3
# Managing Administrators

This chapter provides instructions on creating and managing role-based administrator accounts in Integrity Advanced Server. Before creating administrator accounts, you must create the roles you intend to assign to them.

# Understanding role-based administration

Integrity Advanced Server provides extremely flexible role-based administration capabilities. You can tailor administrator accounts to limit access to specified entities and to specified Integrity Advanced Server functions. This lets you configure administrator accounts that correspond to the division of responsibilities within your organization.

## Understanding access

Administrators are usually responsible for the following tasks:

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

You can assign an administrator to specific entities (user catalogs or groups). If assigned to a catalog, the administrator has access to all groups within that catalog.

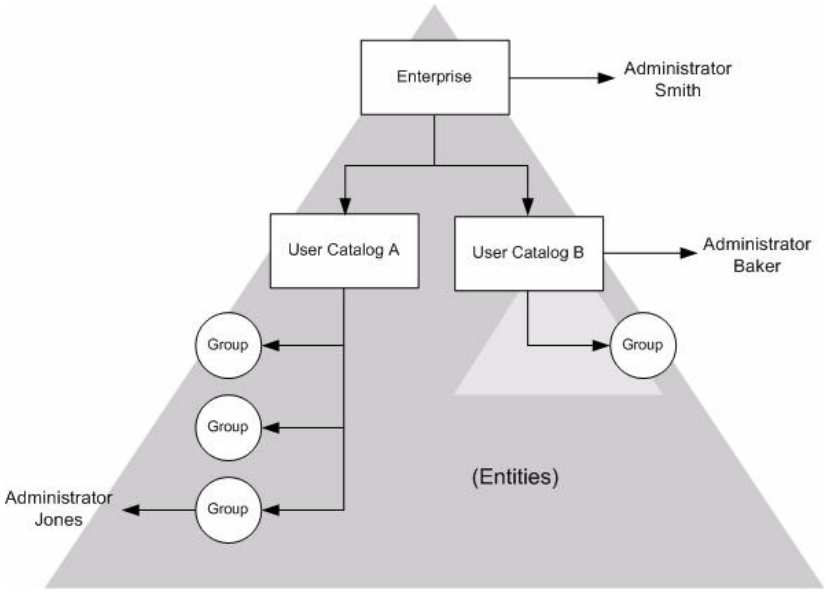



**Figure 3-1:** Administrator Assignment

In the diagram above:

- Administrator Smith has access rights to the whole enterprise and all entities within it. If new entities are added later, Smith will automatically have access to those as well.
- Administrator Baker has access rights to User Catalog B and all groups within it. If new groups are added later, Baker will have access to those as well. Baker has no access to User Catalog A.

- Administrator Jones has access rights only to the group contained within User Catalog C. Jones has no access to any other group.

Role assignment limits the tasks an administrator can perform on assigned entities. For more information, see “Understanding role assignment,” on page 27.

# Understanding role assignment

Each administrator must be assigned a role. Roles are composed of a number of different **privileges** that determine the Integrity Advanced Server features the administrator can access.

If you cannot find a particular feature in the IAS Administration Console, your assigned role may have **no access** to that feature.

## About privileges

You create roles by choosing permission settings for privileges. Privileges correspond to features in the Administration Console.

For each privilege, there are three possible permission settings:

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

## Default roles and customized roles

Integrity Advanced Server comes with six pre-configured roles. These roles are designed to reflect the most common division of administrative tasks.

If the default roles reflect the administrative responsibilities in your organization, simply assign one of these roles to each of your Integrity Advanced Server administrators.

If the default roles do not reflect the administrative responsibilities in your organization, you can edit them by changing their privileges or permissions, or you can create customized roles.

For details about the default roles, see “Using default roles,” on page 29.

For details about creating customized roles, see “Creating customized roles,” on page 30.

### Restrictions and workarounds

Each administrator is assigned to one role.

You cannot assign a role that has greater permissions than your own to another administrator. Make sure you have permission equal to or greater than those you want to assign to another administrator.

You can add only those permissions that your role has to another administrator role.

## Viewing role details

Follow the steps below to view existing roles, and to see what privileges and permissions are given to a particular role.

### To view role details:

1. Choose **System Configuration** | **Administrators**, and click **Manage Roles**.

   The Role Manager page appears, showing all available roles. The list includes default roles, and customized roles.

2. To view the privileges and permissions for a role, click the role name.

For a description of each permission, see “Available privileges,” on page 30.

# Using default roles

Use the information this section to determine whether the Integrity Advanced Server default roles correspond to your organization's administrative structure, and to decide what role to assign to your administrators.

## Administrator default roles

You can assign default roles to administrators or duplicate them to use them as the basis of custom roles. The following default roles are available:

- Master Administrator Role: Has read/write access to all privileges.
- System Administrator Role: Has read/write access to entity, system, and administrator-related privileges. Also has read access to report privileges.
- Customer Administrator Role: Has read/write access to entity, assignment, and administrator-related privileges. Also has read access to policy and report privileges.
- Policy Administrator Role: Has read/write access to all policy-related privileges.

# Creating customized roles

If the default roles do not directly correspond to the division of responsibilities among your administrators, you can create customized roles to control administrator access to Integrity Advanced Server features.

## Available privileges

Listed below are the privileges you can set permissions for when creating a role. For each privilege, you can choose **no access**, **read-only** access, or **read/write** access.

### Privileges

The following table lists the available privileges.

| Access Privilege | An administrator with read/write permission can do the following |
|---|---|
| **System** | |
| Entity Manager | Add, edit, or delete entities in Integrity Advanced Server. |
| Admin Manager | Create administrator accounts, and create, edit, or delete administrator roles. |
| Event Notification | Configure notifications to administrators regarding system events and set up event logs. |
| System Configuration | Configure databases, client settings. |
| Program Advisor | Configure the Program Advisor license and settings. |
| Security Model | Configure the security model. |
| Certificates | Create or delete certificates. |
| **Client Config** | |
| Sandbox | Customize remediation resources. |
| Client Packager | Create a client package to deploy to endpoint computers. |
| **Policy Settings** | |
| Policy Manager | Edit and create security policies. |
| Firewall Rule Management | Create, edit, or delete classic firewall rules, source and destination address profiles, and protocol and port profiles for use in security policies. |
| Enforcement Rule Manager | Create, edit, or delete enforcement rules for use in security policies. Configure a reference client running the anti-virus software to enforce on your network. |
| File Extensions | Edit and create filename extension definitions for use in policy e-mail protection rules and IM Security settings. |

**Table 3-1:** Privileges used to create roles for all administrators

| Access Privilege | An administrator with read/write permission can do the following |
|---|---|
| Program Management | Edit and create program groups for use in security policy program control rules. Import, edit and remove SmartSum reference source files. |
| Anti-Spyware | Edit and create global Anti-Spyware settings, including updating. |
| **Policy Actions** | |
| Policy Assignment | Assign security policies to entities. |
| Policy Deployment | Deploy security policies to the policy server. |
| **Reports** | |
| Reports | Run reports. |

**Table 3-1:** Privileges used to create roles for all administrators

# Creating a customized role

There are two ways to create a new role. You can copy an existing role an modify its settings, or you can create a completely new role.

## Copying an existing role

Follow the steps below to create a new role starting with the permissions of an existing role.

### To create a new role by copying an existing role:

1. Choose **System Configuration** | **Administrators**, and click **Manage Roles**.
2. Select the role you want to copy, then click **Duplicate**.

   The Edit Role page appears.
3. In the privilege row, select **No Access**, **Read,** or **Read/Write**.

You can only modify privileges to which you have Read/Write permissions. Integrity Advanced Server does not display privileges (features) for which you have insufficient permission.

4. Click **Save**.

The new role has been created. You can now assign administrators to this role.

## Creating a role from a blank template

Follow the steps below to create a new role from a blank template.

### To create a new role from a blank template:

1. Choose **System Configuration** | **Administrators**, and click **Manage Roles**.
2. Click **New**.
3. In the privilege row, select **Read** or **Read/Write** to assign permission.

You can only modify privileges to which you have **Read/Write** permissions. Integrity Advanced Server does not display privileges (features) for which you have insufficient permission.

4. Click **Save**.

The role can now be assigned to one or more administrators.

## Modifying an existing role

You can modify a role if your own privileges match or exceed those of that role. You cannot modify your own role.

### To modify a role:

1. Choose **System Configuration** | **Administrators**, and click **Manage Roles**.
2. Select the role you want to modify, then click **Edit**.
3. In the privilege row, select the permission: **No Access**, **Read,** or **Read/Write**.

You can set privileges to which you have Read/Write permissions only. Integrity Advanced Server does not display privileges (features) for which you have insufficient permission.

4. Click **Save**.

Integrity Advanced Server applies the changes the next time administrators assigned that role log on. If any administrators assigned the modified role are already logged on, the administrator must log off and on again to receive the modified role.

# Removing roles

You cannot remove a role that is currently assigned to an administrator. You must assign the administrators to a new role before you can delete the role.

Integrity Advanced Server applies the changes the next time administrators assigned that role log on. If any administrators assigned the modified role are already logged on, the administrator must log off and on again to receive the modified role.

### To remove a role:

1. Choose **System Configuration** | **Administrators**, and click **Manage Roles**.
2. Select the roles you want to remove, then click **Delete**.

   A confirmation box appears listing the roles you are about to delete.
3. Verify that you selected the correct roles, then click **Yes**.

If you attempt to delete an assigned role, an error message appears. You must assign those administrators to a new role before you can remove the role. See “Assigning an administrator to a different role,” on page 35.

The role no longer appears listed on the Role Manager page.

# Configuring administrator accounts

This section describes how to create new administrator accounts, edit existing accounts, and assign roles and entities to an administrator.

## Creating a new administrator account

Before creating a new administrator account, you must know the following information:

- What is the administrator's log in ID and e-mail address?

  If the Integrity Advanced Server administrators are authenticated against an external database, the administrator ID must match the user name in the external database. Furthermore, if external administrator accounts are in different catalogs and administrators can have the same name, append the catalog name before the user name as follows: `catalog.username`.

- Which role do you want to assign to the administrator?

  When you create the account, you must assign the role. Configure the role you will used before creating the account.

- Which entities do you want the administrator to manage?

  You can assign the administrator to one or more specific entities.

## Creating an administrator account

To create an administrator account, you must have administrative privileges greater or equal to the administrator account you are creating.

### To create a new administrator account:

1. Choose **System Configuration** | **Administrators**.
2. Click **New**.
3. In the **Administrator ID** field, type the log on ID for the Administrator.
4. Fill in the remaining fields.
5. In the **Assigned Role** list, click **Edit**.

   The Assign Role page appears.
6. Select a role, click **Save**.

   The role appears in the administrator's current role list.
7. If you wish to restrict the administrator to certain entities, in the **Assigned Entity** list, click **Edit**.

   The **Assign Entities** page appears.

8. Select the entities to restrict the administrator's access to specific user catalogs or groups.

Administrators that are assigned to specific entities can assign policies to only those entities.

9. Click **Save**.

   A list of entities appears in the Current Entities list.

10. Click **Save**.

The administrator account is added.

# Editing an administrator account

To make changes to an administrator account, your role must have privileges equal to or greater than the role of the account you want to change.

### To edit an administrator account:

1. Choose **System Configuration | Administrators**.
2. From the list of administrators, select the administrator account you want to edit, then click the **Edit** button.
3. Make your changes, then click **Save**.

If more than one administrator is selected, the Edit button is unavailable. Be sure you have selected only one administrator.

## Assigning an administrator to a different role

This section explains how to change an administrator's role.

### To assign an administrator to a different role:

1. Open the Administrator Manager page as described above.
2. Select an administrator and click **Assign Role**.
3. Select the new role, then click **Save**.

Integrity Advanced Server applies the changes the next time administrators assigned that role log on. If any administrators assigned the modified role are already logged on, the administrator must log off and on again to receive the modified role.

## Assigning an administrator to different entities

You can change the user catalogs and groups an administrator has access to by editing the administrator account.

### To assign an administrator to different entities:

1. Access the **Edit Administrator** page as described above.
2. Under **Assigned Entities**, click the **Edit** button.
3. Select the new entities, then click **Assign**.
4. Click **Save**.

## Removing an administrator account

If the administrator is logged on when you remove the account, they are automatically logged off.

### To remove an administrator account:

1. Choose **System Configuration** | **Administrators**.
2. Select the administrator accounts you want to remove, then click **Delete**.

   The account is removed from the system.

# Chapter 4
# Managing Policies

Creating and distributing security policies is the core task involved in implementing security with Integrity Advanced Server. This chapter provides an overview of how security policies work, and provides some guidelines for creating effective policies.

The chapter contains a sample policy lifecycle that you can adapt for use in your enterprise, or use as a starting point for understanding key steps in the policy creation process.

# Security policies

An Integrity Advanced Server security policy is a set of rules and settings that governs the behavior of Integrity clients installed on computers connected to a corporate network. There are two policy types that Integrity clients can enforce: **enterprise** and **personal**. (Packaging two enterprise policies together further refines enterprise policies into two sub-types; **connected** and **disconnected**.) Each type contains (with a few exceptions) the same types of security rules, and when enforced by the Integrity client their settings are **arbitrated**.

## Enterprise policies

An enterprise policy provides centralized management of endpoint security. It is defined by an administrator within Policy Manager and assigned to entities. An enterprise policy is enforced when the protected computer is connected to the enterprise network. Depending on settings chosen by the administrator in the enterprise policy itself, it can also be enforced when the computer is not connected to the enterprise network.

Enterprise policies are enforced by both Integrity Agent and Integrity Flex.

### Enterprise policy packages

Create a policy package when you want to centrally manage endpoint security using different enterprise policies for when the computer is connected to or disconnected from the enterprise network.

Two deployed enterprise policies can be packaged together to create a policy package. Each enterprise policy is assigned a role within the package; either as a connected or disconnected policy. The policy package is defined by an administrator within Policy Manager and assigned to entities.

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

Once two enterprise policies are packaged together, if one or the other policy is redeployed, then the policy package is modified and automatically redeployed. The auto-redeploy of the policy package triggers the assigned entities to download the updated policy package.

#### The connected enterprise policy

The connected enterprise policy is enforced when the protected computer is connected to the enterprise network. The connected policy arbitrates with the endpoint personal policy. The connected enterprise policy is no longer enforced when the Integrity client disconnects from the network, even if the **Enforce this policy when client is disconnected** option is selected in the policy.

Connected enterprise policies are enforced by both Integrity Agent and Integrity Flex.

### The disconnected enterprise policy

The disconnected enterprise policy is enforced when the protected computer is disconnected from the enterprise network. The disconnected policy arbitrates with the endpoint personal policy. The disconnected enterprise policy is no longer enforced when the Integrity client connects to the network.

Disconnected enterprise policies are enforced by both Integrity Agent and Integrity Flex. If you deploy a policy package to an Integrity Agent for Linux, the disconnected policy within the policy package will be ignored. Integrity Agent for Linux will only take the connected enterprise policy. Use the RPM Package builder to configure a disconnected policy for Integrity Agent for Linux. For more information, see the Integrity Agent for Linux Installation and Administration Guide.

## The personal policy

The personal policy gives some control over security management to the user of the protected computer, who defines the policy using the Integrity Flex Control Center (user interface).

The personal policy is installed with the Integrity client by default. It can be configured using the `-config` command line parameter.

The personal policy is enforced by the client at all times, unless the administrator configures the enterprise policy to override the personal policy.

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

## Policy arbitration

Integrity Flex **arbitrates** between personal policy and enterprise policy settings, enforcing the most restrictive rules from each policy. For example, if the enterprise policy is configured to allow inbound traffic on port 135, but the personal policy is configured to block it, the traffic will be blocked. Such traffic will also be blocked if

the personal policy is configured to allow it, and the enterprise policy is configured to block it.

### Arbitration options

If you deploy Integrity Flex to your protected computers, you have a range of options to control how the enterprise policy and personal policy will be arbitrated. These options are set in the enterprise policy itself. You can:

- Use the Trusted Zone definitions from only the enterprise policy and arbitrate all other settings. This gives you exclusive power to decide what network entities to treat as trusted.
- Enforce the enterprise policy when the Integrity client is disconnected from the enterprise network. The enterprise policy settings are arbitrated with the personal policy settings.

The **Enforce this policy when client is disconnected** option is not available with policy packages.

- Permit or prevent the user from shutting down the Integrity client when the enterprise policy is being enforced or not enforced.
- Enforce only the enterprise policy, ignoring personal policy settings, when the enterprise policy is being enforced.

Set policy arbitration options in the Client Settings tab in Policy Manager.

# Overview of policy rules

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

This section describes the types of security rules that make up enterprise and personal policies. The following section explains how the different rules are evaluated by Integrity clients, and which rules take precedence in different situations.

## Classic Firewall Rules

Classic firewall rules take a traditional perimeter firewall approach to securing the endpoint, operating independently of session information and program rules. Classic firewall rules are the first type of rule applied to incoming traffic and the last type of rule applied to outgoing traffic; hence they make up your first line of defense against Internet threats.

Classic firewall rules (referred to as “expert rules” in the Integrity Flex user interface and user manual) can block or allow traffic by source/destination addresses, ports, protocols, message types, or time of day.

Classic firewall rules can also be ranked to create a “stack” of rules that the client will evaluate in order, executing the first one that matches the traffic in question.

## Malicious Code Protection

The Integrity client Malicious Code Protection (MCP) feature protects endpoint computers from malicious code arriving in network traffic. MCP can monitor inbound, outbound, or dual-direction network traffic only for the protocols on the ports specified in Table 4-1: MCP monitored ports and protocols.

| Protocol | Description | Port |
|---|---|---|
| FTP | File transfer protocol | 21 |
| HTTP | Hyper Text Transfer Protocol | 80, 591, 8008, 8080, and 11523 |
| IMAP4 | Internet Messaging Access Protocol 4 | 143 |
| NNTP | Network News Transfer Protocol | 119 |
| POP3 | Post Office Protocol 3 | 110 |
| SMTP | Simple Mail Transfer Protocol | 25 |

**Table 4-1:** MCP monitored ports and protocols

MCP is designed to protect against malicious code delivery through network traffic, for example, buffer overflow exploitation. MCP recognizes attacks without requiring a signature of a known attack.

Most malicious code attacks contain executable code in the network payload to run on the target computer. Executable code is normally not allowed to traverse a network, with the exception of a few well known cases, such as an FTP transfer of an executable (.exe) file. Executable code can be identified and characterized more efficiently with an actual examination of the disassembled executable code (machine assembly language). MCP monitors data streams and looks for any binaries it can translate into machine assembly language. This indicates the possible existence of malicious code passing through a network as network traffic usually does not contain executable code.

MCP is able to distinguish between the random "noise" of assembly-like data and a real executable in network traffic. Of course the existence of executable code does not mean it is malicious code. The MCP feature provides the administrator with the flexibility to choose how the identified executable code is to be handled.

### Using the MCP feature

You implement the MCP feature though the security policy. The MCP configuration UI is located on the SmartDefense tab of the Edit Policy page. When you create a security policy, you can turn the MCP feature on or off. Additionally, if you turn MCP on, you need to select the MCP action to observe or act upon MCP events. You can set MCP to monitor inbound, outbound, or dual-direction network traffic for each supported network protocol provided it travels on specific ports, see Table 4-1: "MCP monitored ports and protocols," on page 41.

Use the Client Setting tab of the Edit Policy page to set whether or not MCP events should be logged and uploaded to Integrity Server, which displays the MCP events in the Client Events, Event Details, and User Details reports.

## Zone rules and program rules

Unlike classic firewall rules, Zone rules and program rules take session information into account and operate in conjunction with each other. Traffic is blocked or allowed according to the zone (Trusted, Internet, or Blocked) that the traffic came from or is addressed to, and according to the program that is sending or receiving the traffic.

For a discussion of Zones, see "What are Zones?," on page 68.

## MailSafe rules

The Integrity client MailSafe feature provides protection for both inbound and outbound e-mail. Inbound protection prevents potentially harmful e-mail attachments from affecting the endpoint computer by quarantining them until they are approved. This feature consists of a MailSafe Extensions Manager and policy-specific MailSafe Rules. Outbound protection puts limits on outgoing e-mail to prevent e-mail worms and other malicious code from using the endpoint computer to send messages.

Note that inbound MailSafe protection works with POP3 and IMAP4 protocols, while outbound MailSafe works with SMTP protocol only.

# Enforcement Rules

Enforcement rules establish requirements for a secure environment on the protected computer. If a protected computer does not comply with one or more of these rules, the client is restricted to the sandbox until it becomes compliant.

You can create enforcement rules based on the following conditions:

- **Registry keys and values**. You can specify that certain registry keys an values must (or must not) exist on the protected computer in order for it to be compliant.
- **Files and properties**. You can specify that certain files must be present (or absent) on the protected computer, and also require or prohibit specific file properties, such as version number. In the case of executables, you can require that a program always be running, or immediately restrict the user if an unwanted program launches.
- **Anti-virus provider information**. You can specify that the endpoint be running a specific type of anti-virus software, and specify conditions ensuring up to date virus definition files and anti-virus engine.

## User support considerations for enforcement rules

Enforcement rules are unique because if protected computer isn't in compliance with a rule, the user session is restricted to the sandbox. The user is prevented from accessing any other protected network resources until the endpoint computer becomes compliant. It is very important that the user have access to adequate remediation resources to become compliant and be released from restriction.

For more information, see "Policies: Restricting Non-Secure Endpoints" on page 109.

# Rule evaluation and precedence

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

## How traffic is evaluated

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

### Hard-coded rules

You can configure the following hard-coded rules in the Integrity Advanced Server configuration file:

- Allow UDP (User Datagram Protocol) packets to and from the Integrity Advanced Server port 6054
- Allow UDP  packets to and from the Integrity Advanced Server port 443
- Allow traffic from the local machine to port 53 on any computer

  This rule allows access to the Domain Name Service.
- Accept ICMP (Internet Control Message Protocol) type 9 to local machine

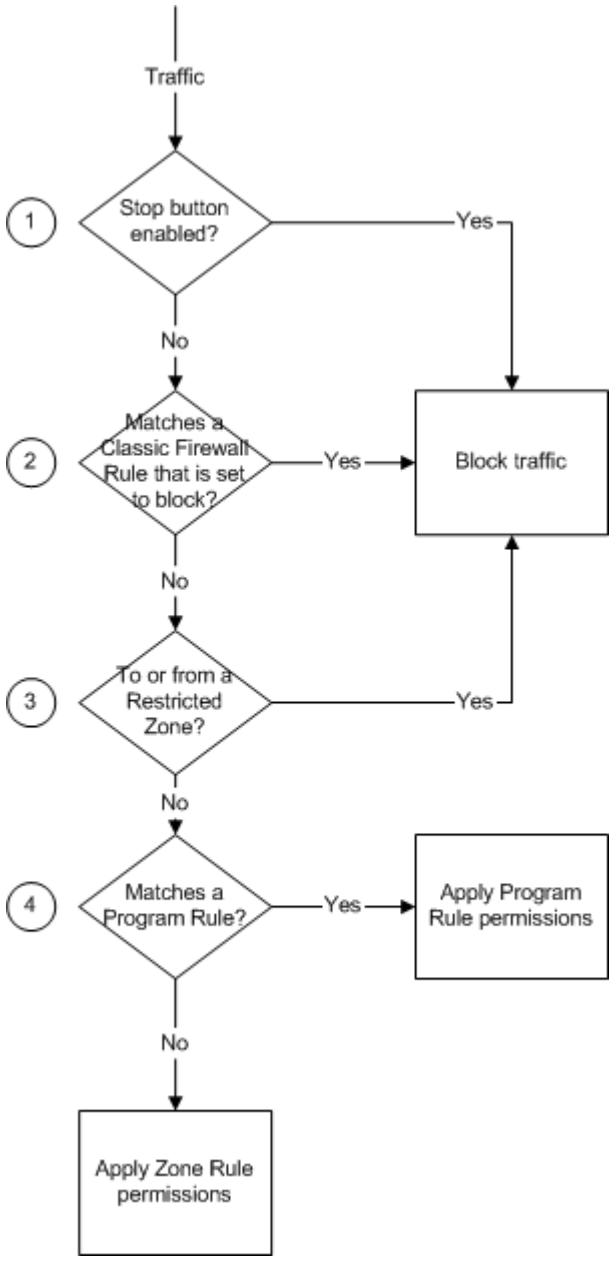
  This rule allows router advertisement.
- Block all traffic from sources which is not in the Trusted or the Internet Zone

  This rule is the ‘cleanup rule’, which blocks all unhandled traffic.

### Policy rules

The diagram below shows how Integrity client evaluates the security rules for network traffic.

**Figure 4-1:** Rule evaluation for incoming and outgoing traffic




Integrity client checks hard-coded firewall rules before evaluating traffic against the enterprise or personal policy rules. The system administrator controls the following hard-coded rules in the Integrity Advanced Server configuration file:

- Allow UDP (User Datagram Protocol) packets to and from the Integrity Advanced Server port 6054
- Allow UDP  packets to and from the Integrity Advanced Server port 443

- Allow traffic from the local machine to port 53 on any computer (Domain Name Service)
- Accept ICMP (Internet Control Message Protocol) type 9 to local machine (router advertisement)
- Block all traffic from to or from sources which is not in the Trusted or the Internet Zone

If the traffic is allowed by these rules, Integrity client then verifies the traffic against the policy in the following order:

1. the Integrity client checks for the Stop button.
    - If the endpoint user is using Integrity Flex, and has enabled the stop button to stop all traffic, the traffic is blocked.
    - If the stop button is not enabled, the evaluation process proceeds to the next step.
2. The Integrity client checks for a matching Classic Firewall Rule.
    - If the Classic Firewall Rule defined in the policy says to block this traffic, the traffic is blocked.
    - If there is no Classic Firewall rule blocking this traffic, the evaluation process proceeds to the next step.
3. The Integrity client checks if the traffic is going to or coming from a restricted Zone.
    - If the traffic comes from, or is going to a Zone that is defined as restricted, the traffic is blocked.
    - If the traffic does not come from or going to a restricted Zone, the evaluation process proceeds to the next step.
4. The Integrity client checks for applicable program rules
    a. If the traffic matches a program rule in the policy, the Integrity client applies that program rule.
    b. If the traffic does not match any program rules, the Integrity client applies the Zone rule.

# Managing policies

This section explains how to use policy templates and Policy Manager to create, edit, and delete security policies.

The following topics are covered:



## Integrity Advanced Server pre-configured policy templates

Integrity Advanced Server includes pre-configured policy templates. This section describes the templates.

Integrity Advanced Server ships with the following pre-configured policy templates:

- **Observation** is designed for observing endpoint behavior and testing Integrity client deployment. The policy sets the security level for the Trusted and Internet Zones to Low, allowing unrestricted traffic and maximum functionality. Unknown programs can access the network as either clients or servers. Connectivity alerts let administrators confirm connections to the server. It is recommended to turn off connectivity alerts before general deployment.
- **Medium Security** provides medium security with minimal end-user interruptions. To allow maximum functionality, the policy adds newly-detected network locations to the Trusted Zone. Flex users can add locations to their personal Trusted Zones. Unknown programs can access the network as clients, though they cannot act as servers. It is recommended to define programs or to use Program Advisor with this policy.
- **High Security** provides high security and, by default, a high number of end-user alerts. The policy adds newly-detected network locations to the Internet Zone and sets the security level for that zone to High. Because these settings can block communications from legitimate sources, you should add such sources to the Trusted Zone before deploying the policy. Flex users can add locations to their personal Trusted Zones, so it is recommended to deploy Integrity Agent to users who should not have this ability. Program Control is configured to block unknown programs from accessing the network. It is therefore important to define programs or to use Program Advisor with this policy. The policy turns on a high number of alerts for evaluation purposes. To minimize user interruptions, disable all alerts other than enforcement alerts before general deployment.

## Creating a new security policy

Before you create a new security policy, you can first create new security rules to include in the security policy. You can also add these security rules to the policy at a later time. See "Editing a security policy" on page 49.

### To create a new security policy from a template:

1. Go to **Policies**.

   The Policy Manager page appears.

2. Click **New**, and select **From Template**

   The Create New Policy page appears.

3. In the **Policy Name** box, type a name for the new policy.

4. Select the policy template to use, then click **Create**.

   The Edit Policy page appears with a message indicating the new policy was created successfully.

5. Navigate through the various tabs to edit or add the security rules and settings:

   a. Select the **Lock this policy** check box, if you want to be the only administrator to change this security policy.

   b. Click **Save**.

   The Version Comments page appears.

6. In the **Comment** box, type comments to indicate the changes made in this version of the policy. Comments help identify major changes in case a roll back is needed later. Comments longer than 150 characters will be truncated.

7. Either save the new policy or save and deploy the new policy.

   - Click **Save** to save the policy to continue work on it later.
   - Click **Save & Deploy** to save the new policy and deploy it to the policy server. Deploying the new policy makes it available for assignment to an entity.

   The Policy Manager page appears with a message indicating the policy was saved successfully.

### To create a new security policy from a file:

1. Go to **Policies**.

   The Policy Manager page appears.

2. Click **New**, and select **From File**.

   The Import Policy page appears.

3. In the **Policy Name** box, type a name for the new policy.

4. Click **Browse** to navigate to the XML policy file to import, then click **Import**.

   The Edit Policy settings page appears with a message indicating the new policy was created successfully.

5. Navigate through the various tabs to edit or add the security rules and settings:

   a. Select the **Lock this policy** check box, if you want to be the only administrator to change this security policy.

   b. Click **Save**.

   The Version Comments page appears.

6. In the **Comment** box, type comments to indicate the changes made in this version of the policy. Comments help identify major changes in case a roll back is needed later. Comments longer than 150 characters will be truncated.

7. Either save the new policy or save and deploy the new policy.

   - Click **Save** to save the policy to continue work on it later.
   - Click **Save & Deploy** to save the new policy and deploy it to the policy server. Deploying the new policy makes it available for assignment to an entity.

   The Policy Manager page appears with a message indicating the policy was saved successfully.

Some attributes are not imported, including gateway locations and destinations, and any attribute that cannot be set using the Integrity Advanced Server Administrator Console. Some attributes are also overwritten.

# Editing a security policy

Before editing a security policy, check the security policy's usage. A policy can be assigned to one or more entities and included in one or more policy packages or client packages.

### To edit a security policy:

1. Go to **Policies**.

   The Policy Manager page appears.

2. Select the policy to edit, then click **Edit**.

   The Edit Policy page appears.

3. On the Edit Policy settings page, do the following:

   a. Navigate through the various tabs to edit or add the following rules and settings:

      - Firewall rules
      - Zone rules
      - Program rules
      - SmartDefense
      - MailSafe rules

- Enforcement settings
- Client settings

For more details about creating and adding these rules and settings to a security policy, see chapters 5 through 11.

**b.** Select the **Lock this policy** check box, if you want to be the only administrator to edit this security policy.

**4.** Click **Save**.

The Version Comments page appears.

**5.** In the **Comment** box, type comments to indicate the changes made in this version of the policy. Comments help identify major changes in case a roll back is needed later. Comments longer than 150 characters will be truncated.

**6.** Either save the new policy or save and deploy the new policy.

- Click **Save** to save the policy to continue work on it later.
- Click **Save & Deploy** to save the new policy and deploy it to the policy server. Deploying the new policy makes it available for assignment to an entity.

The Policy Manager page appears with a message indicating the policy was saved successfully.

# Deleting a security policy

You cannot delete a policy that is assigned to an entity or included in a client package. Before deleting a policy, search for any entities to which the policy is assigned and then assign a different policy to those entities (or set them to inherit their parent entity's policy). After changing the policy assignment, delete the old policy.

### To delete a policy:

**1.** If you are sure the policy is not assigned to any entities, skip to step 7.

If the policy is (or might be) assigned to any entities, choose **Entities**.

The Entity Manager page appears.

**2.** Click  to display the Search box.

**3.** In the Search box, select the relevant policy from the **With assigned policy** dropdown list and click **Search**.

Integrity returns the list of entities to which that policy is assigned.

**4.** Select all entities in the list and click **Assign Policy**.

The Policy Assignment screen appears.

5. In the **Policy** dropdown list, select a new policy (or select **Inherit from parent**).
6. Click **Assign**.

   If you have more entities than one page can accommodate, page through the entities and repeat steps 4 through 6 as necessary.
7. Go to **Policies**.

   The Policy Manager page appears.
8. Select the policy to delete and click **Delete**.

   A confirmation message appears.
9. Click **Yes**.

# Managing policy packages

This section explains how to use the Policy Manager to create, edit, and delete policy packages.

## Creating a new policy package

Before you create a new policy package, you must create and deploy the enterprise security policies to include in the policy package. See “Creating a new security policy” on page 47.

### To create a new policy package:

1. Go to **Policies**.

   The Policy Manager page appears.

2. Click **New**, and select **Policy Package**.

   The New Policy Package page appears.

3. In the **Name** box, type a name for the new policy package.

4. In the **Connected Enterprise Policy** drop-down list, select a policy to use when the endpoint computer is connected to the enterprise network.

5. In the **Disconnected Enterprise Policy** drop-down list, select a policy to use when the endpoint computer is disconnected from the enterprise network.

6. Click **Save**.

   The Policy Manager page appears with a message indicating the policy package was created successfully.

## Editing a policy package

Before editing a policy package, check the policy package’s usage. A policy package can be assigned to one or more entities and included in one or more client packages.

### To edit a policy package:

1. Go to **Policies**.

   The Policy Manager page appears.

2. Select the policy package to edit, then click **Edit**.

   The Edit Policy Package page appears.

3. In the **Name** box, edit the name to change the policy package name.
4. In the **Connected Enterprise Policy** drop-down list, select a different policy to use when the endpoint computer is connected to the enterprise network.
5. In the **Disconnected Enterprise Policy** drop-down list, select a different policy to use when the endpoint computer is disconnected from the enterprise network.
6. Click **Save**.

   The Policy Manager page appears with a message indicating the policy package was updated successfully.

# Deleting a policy package

Before deleting a policy package, make sure the policy package is not assigned to any entities. You cannot delete an assigned policy package or a policy package that is included in a client package.

### To delete a policy package:

1. Go to **Policies**.

   The Policy Manager page appears.
2. Select the policy package to delete, then click **Delete**.

   A message appears asking if you are sure you want to delete this policy package.
3. Click **Yes**.

   The Policy Manager page appears with a message indicating the policy package was deleted successfully.

# A model policy lifecycle

This model lifecycle starts with the assumption that there is no current emergency which would require you to immediately impose very strict security rules. In the trade-off between unknown attack protection, user restriction, and policy maintenance requirements, it begins with an emphasis on low restriction and low maintenance, and moves iteratively in the direction of higher unknown attack protection and higher user restrictions.

## Policy 1: Discovery Mode

In the initial policy deployment, you will use classic firewall rules to block only particular ports associated with known vulnerabilities. The primary purpose of the first policy is to gather information you will use to establish program rules, Zone rules, or further classic firewall rules.

### To create and deploy the first policy:

1. Create a policy from the Observation policy template.
2. Add classic firewall rules.
   a. Block particular ports associated with known vulnerabilities.
   b. Create a rule explicitly allowing and tracking all other ports. This rule will generate entries in the Firewall Event report showing in detail each endpoint's network communications. You can use this information to determine what IP addresses, ranges, hosts, and subnets need to be put in the Trusted Zone.
3. Deploy the first policy.

## Policy 2: Define known programs, Trusted Zone elements, and initial program rules

When you feel you have collected enough information to populate the majority (if not the entirety) of your Trusted Zone, it's time to create and deploy the second policy.

In your second policy, you begin creating program rules and defining your Trusted Zone. Using a program reference scan, you selectively block and allow specific applications, and also prevent unknown applications from acting as servers on the Internet.

### To create and deploy the second policy:

1. If you have a tightly-controlled disk image, or a secure, clean computer to use to create program reference sources, create and import a reference source.
2. Create rules for Referenced Programs, in the Program Rules tab in Policy Manager. In general, the more secure your reference machine, the more safely you can grant referenced programs access or server rights.
3. If you do not have a tightly-controlled disk image, or for other reasons you need to discover programs in use on your network that you may want to allow or block, use

the Program Details Report and Program Manager to review applications captured by Program Observation. Focus on distinguishing two types of programs:

**a.** Programs to which you may want to give access or server rights, but which do not exist on your reference computer.

**b.** Programs to which you want to deny access or server rights because of known vulnerabilities.

**4.** To simplify rule assignments, create program groups for similar programs that you want to grant similar permissions to. For example, if you know you want to allow all common browsers in use on your network, you might create a Browsers program group. Similarly, if you want to block instant messaging programs, you might create a group containing all observed instant messaging programs.

**5.** Create rules allowing or blocking the program groups you have created, or individual programs. Use the Specific Programs and Program Groups area in the Program Rules tab.

**6.** Create rules for unknown programs, using the All Other Programs area of the Program Rules tab. For guidance in creating unknown program rules, see “Choosing All Other Programs Rules” on page 95.

**7.** Use the Firewall Events Report in the Reporting module of Integrity Advanced Server, or your own knowledge of your network structure, to add necessary network elements to the Trusted Zone. A simple approach is to add your entire local network now, then gradually tighten the Zone (that is, reduce the scope of trusted elements) in later iterations.

**8.** Set the Security Level for Trusted Zone and Internet Zone.

**a.** Go from Low/Low to Medium/Medium.

**b.** Block fragmented packets.

The “Block fragmented packets” setting is recommended only for internally connected machines. VPN and dial-up connections result in fragmented packets fairly frequently, so blocking fragments in a policy assigned to users with those connections could cause problems.

**9.** Add any further classic firewall rules you need.

**10.** Deploy the policy.

## Policy 3 and subsequent: Refine Trusted Zone and Program Rules

In the third policy iteration, and in subsequent iterations, you begin to refine your program rules. In the second policy, you blocked or allowed specific known applications, while allowing most kinds of traffic by unknown programs. In the third policy (and future policies), you further tighten restrictions on unknown applications, while continuing to add to your list of allowed applications as necessary.

### To create and deploy the third policy:

1. Continue to use Firewall reports to identify network elements that need to be in the Trusted Zone, and add those elements to the Zone. This is very important at this stage, because by raising the security level for the Internet Zone to High (step 4 below) you will greatly restrict the types of traffic endpoints can receive from hosts in the Internet Zone. If you have begun by trusting your entire local network, consider tightening the Zone by removing ranges or subnets that may not need to be trusted.
2. Use Program Manager to identify additional non-referenced programs you want to allow. Add them to the groups you created for the second policy, or assign permissions to them individually.
3. When you're satisfied that you have a fairly comprehensive listing of the programs you want to allow from reference sources, program observation, or both, and you've set up the rules for those programs to your satisfaction, make the rules for unknown programs more strict. Again, use the criteria discussed in "Choosing All Other Programs Rules" on page 95.

Remember that the success of your program control rules depends on accurate definition of your Trusted Zone.

4. Adjust the Security Level for the Trusted Zone and Internet Zone.

   Set security to High (Internet Zone) and Medium (Trusted Zone).
5. Deploy and continue to update this policy as needed.

# Chapter 5
# Policies: Classic Firewall Rules

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

Use classic firewall rules to:

- Create a standard perimeter firewall on the protected computer. See "Using classic firewall rules in security policies," on page 63.
- Fine-tune program control by restricting the network access of a program or program group. Chapter 7 Policies: Program Control.

# Understanding classic firewall rules

Classic firewall rules block or allow network traffic based on attributes of communication packets. You can use classic firewall rules to block or allow traffic based on the following three attributes:

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

## Defining source and destination locations

Before you can create a classic firewall rule that allows or blocks traffic by location, you must define the location in the Location Manager. Locations can be an IP address, subnet, or range of addresses.

## Defining protocols and ports

Before you can create a classic firewall rule that allows or blocks traffic by protocol or port, you must define the protocol or port in the Protocol and Port Manager. Protocols are used to refine firewall rules to match traffic based on network protocol and ports. Protocols can be a IP network protocol or ICPM/IGM message types and port numbers can be used for protocols which support port addressing.

## Classic firewall rank in security policies

In a security policy, rank is the order in which Integrity client evaluates and executes the classic firewall rules. Because Integrity client executes the first rule to match only, the rule's rank is extremely important.

### Example of FTP access

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

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

#### Example 1: Allow local traffic and block other traffic

**Figure 5-1:** Example with FTP Local rule rank 1

| Rank | Name | Source | Destination | Protocol | Time | Action | Track |
|---|---|---|---|---|---|---|---|
| 0 | FTP Local | Private Subnet | Any | IP_TCP_UDP | Always | Allow | Log |
| 1 | FTP Internet | Any | Any | IP_TCP_UDP | Always | Block | None |

In the first example, FTP Local is rank 1 and FTP Internet is rank 2.

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

### Example 2: All access is blocked

**Figure 5-2:** Example with FTP Internet rule rank 1

| Rank | Name | Source | Destination | Protocol | Time | Action | Track |
|---|---|---|---|---|---|---|---|
| 0 | FTP Internet | Any | Any | IP_TCP_UDP | Always | Block | None |
| 1 | FTP Local | Private Subnet | Any | IP_TCP_UDP | Always | Allow | Log |

In the second example, FTP Internet is rank 1 and FTP Local is rank 2.

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

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

# Managing classic firewall rules

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

## Creating a new classic firewall rule

Before you can add a classic firewall rule to a policy, you must create the rule in the Classic Firewall Rule Manager.

### To create a new rule:

1. Go to **Policy Objects** | **Firewall Rules**.

   The Classic Firewall Rule Manager page appears.

2. Click **New**.

   The New/Edit Classic Firewalll Rule page appears.

3. Complete the general information.

   a. In the **Name** box, type a name for the rule.

   The name must be unique and is limited to 128 characters.

   b. In the **Description** box, type a description of the rule.

   The description is limited to 250 characters.

   c. In **Action**, select:

   - **Allow** to create a rule that grants access when the rule conditions are met
   - **Block** to create a rule that denies access when the rule conditions are met

   d. In **Track**, select:

   - **None** to neither log the event nor alert the endpoint user of the activity. When tracking is set to none, rule usage does not appear in the reports.
   - **Log** to record activity without alerting the endpoint user of the activity.
   - **Alert and log** to record activity and display a pop-up on the protected computer when activity occurs.

Tracking (alerts and/or logging) occurs when Integrity client executes the rule.

4. Add source or destination locations to the rule. To set the location to Any, leave the source or destination location blank.

   Perform the following steps to add a source:

   a. In **Source**, click **Add**.

   The **Add Sources to Firewall Rule** page appears.

**b.** Select a location, then click **Add**.

Perform the following steps to add a destination:

**a.** In **Destination**, click **Add**.

The **Add Destinations to Firewall Rule** page appears.

**b.** Select a destination, then click **Add**.

5. Add a protocol or port to the rule. To set the protocol to Any, leave the protocol type blank.

**a.** In **Protocol**, click **Add**.

The **Add Protocol to Firewall Rule** page appears.

**b.** Select a protocol, then click **Add**.

6. Click **Save**.

Now you can add this classic firewall rule to a security policy as described in "Adding a classic firewall rule to a security policy," on page 63.

# Editing a classic firewall rule

You can change the settings of an existing rule. When you modify a rule, the rule settings in all the security policies that include it are automatically updated. However, the policies must be re-deployed before the changes affect the endpoint users. The following instructions explain how to modify a rule and update the endpoint users policy.

### To modify a rule and deliver an updated policy:

1. Go to **Policy Objects** | **Firewall Rules,** then change the rule settings.

For detailed instructions see "Creating a new classic firewall rule," on page 60.

2. Go to **Policies**.

The Policy Manager page appears. The modified icon appears in the policy list next to policies that were updated but not deployed.

3. Verify that the policy has the classic firewall rule that you changed.

**a.** In the policy list, click the **policy name**.

The View Policy Settings page appears.

**b.** Go to the **Firewall Settings** tab.

**c.** Verify that the rule is in the policy.

To compare the deployed version to the current version, click the Deployed on date hyperlink to view the deployed version settings.

4. Select the policy, then click **Deploy**.

The current version of the policy is sent to the policy server. Integrity clients that are connected to Integrity Advanced Server download the updated policy on the next heartbeat. Integrity clients that are not connected download the policy the next time the user logs into the system.

# Deleting a classic firewall rule

You can delete a classic firewall rule from the Integrity Advanced Server system, even rules used in security policies. Deleting a rule automatically removes it from all security policies. However, the policies must be re-deployed before the changes affect the endpoint users.

### To delete a rule and deliver an updated policy:

1. Open the Classic Firewall Rule Manager by clicking **Policy Objects** | **Firewall Rules**.

   The Classic Firewall Rule Manager appears.

2. Select a rule, then click **Delete**.

Global classic firewall rules can be deleted from the System Domain only.

3. Click **Yes** to confirm.

   The classic firewall rule is removed from the system.

4. Go to **Policies**.

   The Policy Manager page appears. The modified icon appears in the policy list next to policies that were updated but not deployed.

5. Verify that the policy no longer has the classic firewall rule.

   a. In the policy list, click on the **policy name**.

      The View Policy Settings page appears.

   b. Go to the **Firewall Settings** tab.

   c. Verify that the rule is no longer in the policy.

To compare the deployed version to the current version, click the Deployed on date hyperlink to view the deployed version settings.

6. Select the policy, then click **Deploy**.

Endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat; otherwise endpoint users receive the updated policy the next time they log on.

# Using classic firewall rules in security policies

This section explains how to manage classic firewall rules in a security policy.

## Adding a classic firewall rule to a security policy

Follow the steps below to add a rule created in the Classic Firewall Rule Manager to a security policy. The same Classic Firewall Rule can be assigned to different security policies.

### To add an existing rule to a policy:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.
3. Select the **Firewall Settings** tab.
4. In the Firewall Settings table, click **Add**.

   The Add Classic Firewall Rule to Policy page appears.

Rules that are already in the policy are not listed.

5. Select rules, then click **Add**.

   The Classic Firewall Rule Manager page appears with the rules you selected listed. The rules are automatically ranked and enabled.

If the rule is not added with the correct rank, follow the instructions in “Ranking Classic Firewall Rules,” on page 64.

6. Click **Save**.

   The Version Comments page appears.

7. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

   The Policy Manager page appears. The classic firewall rules are now in the security policy.

8. Select the policy, then click **Deploy**.

Endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat; otherwise endpoint users receive the updated policy the next time they log on.

# Ranking Classic Firewall Rules

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

Before ranking rules, see "Classic firewall rank in security policies," on page 58, for examples of how rank determines the behavior of the Integrity client.

### To change a classic firewall rule's rank:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.
3. Select the **Classic Firewall Rule** tab.
4. Select a rule, then click:

    To move the rule to the top position in the rank.

    To increase the rule's rank by one.

    To decrease the rule's rank by one.

    To move the rule to the bottom position in the rank.

5. After the classic firewall rules are in the correct order, click **Save**.

   The Version Comments page appears.

6. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

   The Policy Manager page appears. The classic firewall rules are now in the security policy.

7. Select the policy, then click **Deploy**.

Endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat; otherwise endpoint users receive the updated policy the next time they log on.

# Enabling and Disabling classic firewall rules

After adding a rule to a policy, you can temporarily disable it without removing it from the policy.

- **Disabled** rules are dimmed. Disabled rules don't affect network traffic.
- **Enabled** rules have a Rank. Enabled rules are evaluated and executed in the rank order, and affect network traffic.

### To enable and disable rules:

1. Open the Policy Manager by clicking **Policies**.

   The Policy Manager page appears.

2. Select a policy, then click **Edit**.

3. Select the **Classic Firewall Rule** tab.

4. To enable or disable the rule, select a rule:

   - Click **Disable**

     The rule's rank is changed to Disabled.

   - Click **Enabled**.

     The rule's rank appears.

5. Click **Save**.

   The Version Comments page appears.

6. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

   The Policy Manager page appears. The classic firewall rules you disabled are now disabled in the security policy.

7. Select the policy, then click **Deploy**.

Endpoint users who are logged on and assigned to the policy receive an update version of the policy at the next heartbeat; otherwise endpoint users receive the updated policy the next time they log on.

## Removing a classic firewall rule from a security policy

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

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

### To remove a rule from a policy:

1. Open the Policy Manager by clicking **Policies**.

2. Select a policy, then click **Edit**.

3. Select the Classic Firewall Rule tab.

4. Select the rule you want to remove, click **Remove**.

5. Click **Save**.

   The Version Comments page appears.

6. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

   The Policy Manager page appears. The classic firewall rules are now in the security policy.

7. Select the policy, then click **Deploy**.

Endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat; otherwise endpoint users receive the updated policy the next time they log on.

# Chapter 6
# Policies: Zone-Based Security

This chapter explains how to use the Integrity Advanced Server's Access Zones and Zone rules features to create security rules in policies that control protected endpoint computer network activity.

# Understanding Access Zones and Zone Rules

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

## What are Zones?

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

### Trusted Zone

The Trusted Zone contains traffic sources that you know and trust. In designing policies, you configure the Trusted Zone to include the network elements your protected computers need to communicate with, such as private subnets and IP ranges of a corporate LAN.

### Blocked Zone

The Blocked Zone contains traffic sources that you don't want your protect computers communicating with at all. In designing policies, you may want to populate the Blocked Zone with dangerous or otherwise undesirable hosts. Blocked sources may include internal hosts or networks.

### Internet Zone

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

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

## How Zone rules work

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

The traffic is allowed if either of the following conditions is met:

- Zone rules allow traffic with the Zone in question via the port or protocol used.
- Program rules allow the program to communicate with the Zone in question via the port or protocol used.

Classic firewall rules take precedence over Zone rules. For more information, see "Rule evaluation and precedence," on page 44.

# Workflow for Zone-based security

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

1. Configure the Trusted Zone.

   Research your network setup to see which subnets, hosts, or other resources need to be trusted, then create location definitions and add them to the Trusted Zone. See "Configuring the Trusted Zone," on page 70.

2. Configure new network detection options.

   Determine Integrity clients behavior when they detect an unfamiliar network. See "Configuring new network detection options," on page 72.

3. Configure Zone rule settings.

   After you have defined your policy's Zones, configure Zone settings to specify traffic that is allowed for the Trusted and Internet Zones. See "Using Zone Rules in a security policy," on page 73.

4. Add new trusted and blocked locations as they are identified.

   Over time, you will identify new computers and networks to either trust or block. Incorporate them into your setup by creating new locations and adding them to the appropriate Zones.

# Managing access Zones in a security policy

This section explains how to set up access Zones in security policies. Configuring Zones allows you to set up both Zone and program rules.

## Configuring the Trusted Zone

One of the key tasks involved in creating successful Integrity policies is to carefully populate the Trusted Zone with resources your protected computers need.

### Planning Trusted Zone contents

Initially, you may not know exactly what to put in the Trusted Zone. As a starting point, you can add all subnets and IP ranges of your corporate network to the Trusted Zone, thereby giving all your endpoints easy access to all elements of your network. This has the advantage of low user impact, as users will continue to have access to all the network resources they need. However, this approach does not provide the highest level of protection.

As you create successive policies during the policy lifecycle, refine the contents of the Trusted Zone by specifying the hosts that need to be trusted, and removing subnets or ranges in your network that your users don't need such easy access to. The goal is to create a Trusted Zone that contains only those network elements your endpoints truly need to trust.

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

The table below lists elements that typically need to be trusted.

| Resources | Description |
|---|---|
| Required | Remote host computers connected to the protected computer (if not included in the subnet definitions for the corporate network) |
| | Corporate Wide Area Network (WAN) subnets that will be accessed by the protected computer |
| | Corporate LANs that will be accessed by the protected computer |
| | Integrity Advanced Server |

**Table 6-1:** Trusted resources

| Resources | Description |
|---|---|
| Possibly Required | DNS servers |
| | Local host computer's NIC loopback address (depending on Windows version). If you specify a local host loopback address of 127.0.0.1, do not run proxy software on the local host. |
| | Internet gateways |
| | Local subnets |
| | Security servers (for example, RADIUS, ACE, or TACACS servers) |

**Table 6-1:** Trusted resources (Continued)

## Creating locations for trusted elements

After you have determined which elements you want to add to the Trusted Zone, use the Location Manager to create definitions of those elements.

## Adding locations to the Trusted Zone

After you have created locations, follow the steps below to add locations to the Trusted or Blocked Zones for the security policy. The Zones are set up separately for each security policy.

### To set up a security policy's access Zones:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.
3. Select the **Access Zones** tab.
4. In the Locations and Zones area, click **Add**.

   The Add Locations to Zone page appears.
5. In the **Add items to** drop-down list, select the location's Zone.
6. Select a location, then click **Add**.
7. Click **Save**.

   The Version Comments page appears.
8. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

The Policy Manager page appears. The access Zones are now configured.

# Configuring new network detection options

New network detection options determine what the Integrity client does when the protected computer connects to a network that has not already been placed in the Trusted Zone or Internet Zone.

### To set up a security policy's access Zones:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.
3. Select the **Access Zones** tab.
4. In Network Access Zones for the policy, select one of the following options.
   - **Include the network in the Trusted Zone**. This automatically adds detected networks to the Trusted Zone on the protected computer.
   - **Leave the network in the Internet Zone**. This automatically adds the network to the Internet Zone on the protected computer.
   - **Ask the endpoint user**. This alerts the user that a new network has been detected and asks the user to choose a Zone.
5. Click **Save**.

   The Version Comments page appears.
6. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

The Policy Manager page appears. The access Zones are now configured.

# Using Zone Rules in a security policy

This section explains how to use a Zone rule in security policies. Configuring the Zone rule of a security policy allows you to manage Zone based firewalls on the endpoint user's computer.

## Configuring global packet handling settings

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

### To configure a policy's Zone rules global settings:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.
3. Select the **Zone Rules** tab.
4. In Security Rules for the policy, select the packet types and conditions you want to block.
   - **Block fragment at all security levels**. Blocks incomplete IP packets. When selected the protected computers are completely protected against fragment attacks; however, this functionality is not suitable for users with dial-up connections.
   - **Block VPN protocols (ESP, AH, GRE, SKIP) at High Security.** Blocks the following protocols used by Virtual Private Networks: ESP (Encapsulating Security Payload), AH (Authentication Header), GRE (Generic Route Encapsulation) and SKIP (Simple Key management for Internet Protocols). Because this option can interfere with legitimate traffic on enterprise networks, Integrity client enforces it only for the High security level.
   - **Allow uncommon protocols at High Security.** Allows traffic using uncommon protocols at a high security level. Leave this option cleared unless the protected computers in your network require one or more specialized protocols.
5. Click **Save**.

   The Version Comments page appears.
6. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

   The Policy Manager page appears. The Zone rules are now in the security policy.

## Choosing security levels

To ease administration, Integrity Advanced Server provides three pre-configured security levels that you can apply immediately to the Internet Zone or Trusted Zone.

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

  This level is recommended for the Trusted Zone in security policies for protected computers on a Local Area Network (LAN). Medium security also enforces Program Control.
- **High** security establishes the strongest level of security by restricting most traffic types.

  This level is recommended for the Internet Zone of protected computers connected directly to the Internet or connected via an insecure network (such as a remote user's ISP).

## Refining security level settings

You can refine security level settings by blocking or allowing traffic on specific ports.

### To refine security level settings:

1. In the Zone Rules tab, click the **Advanced** button for either the Internet Zone or Trusted Zone.

   The settings for the currently-selected security level appear.
2. Refine your settings by choosing **Allow** or **Block**. For TCP and UDP, type in port numbers or ranges.
3. When you are finished, click **Hide**, then **Save**.

## Default security level settings

The following table lists the default security level settings.

| Traffic Type | High Security | Medium Security | Low Security |
|---|---|---|---|
| DNS outgoing | Block | Allow | Allow |
| DHCP outgoing | Block | Allow | Allow |
| Broadcast/multicast | Allow | Allow | Allow |
| ICMP | | | |
| Incoming (ping echo) | Block | Allow | Allow |
| Incoming (other) | Block | Allow | Allow |

| Traffic Type | High Security | Medium Security | Low Security |
|---|---|---|---|
| Outgoing (ping echo) | Block | Allow | Allow |
| Outgoing (other) | Block | Allow | Allow |
| IGMP | | | |
| Incoming | Block | Allow | Allow |
| Outgoing | Block | Allow | Allow |
| NetBIOS | | | |
| Incoming | Block | Block/Allow[a] | Allow |
| Outgoing | Block | Allow | Allow |
| **UDP** ports not in used by a permitted program | | | |
| Incoming | Block | Allow | Allow |
| Outgoing | Block | Allow | Allow |
| **TCP** ports not in used by a permitted program | | | |
| Incoming | Block | Allow | Allow |
| Outgoing | Block | Allow | Allow |

a. Incoming NetBIOS traffic is blocked for the Internet Zone.

# Chapter 7
# Policies: Program Control

This chapter explains how to use the Integrity Advanced Server Program Control feature. Use Program Control for the following security tasks:

- Manage risk-mitigating policies that counter malware as well as other invasive threats, such as spyware and adware
- Identify rogue programs that may conflict with system resources
- Establish consistent security policies across the entire enterprise

To require that a protected endpoint computer runs a specific program, such as anti-virus software, use the enforcement feature. (See "Using enforcement rules in a security policy," on page 127.)

Check Point's Program Advisor service streamlines program management by providing professionally-recommended security settings for most programs. If you are using Program Advisor, you will be able to skip most of the topics in this chapter. See "Program Advisor," on page 100 for information about managing programs and program permissions using Program Advisor.

# Understanding Program Control

Program control enables you to create a tiered set of rules that apply different security configurations to the following categories of programs:

- **Specific Programs and Program Groups (Program Control)**. These are programs that Integrity clients have observed on your network, and to which you have assigned specific access rules, either individually or in groups.
- **Referenced Programs.** These are programs listed in reference source files that you have created by scanning a clean, secure computer that has many of the applications commonly in use on your network.
- **All Other Programs**. These are programs that do not exist in reference programs, and to which you have not assigned any access rules.

When a program on a protected computer tries to establish or accept a network connection, the Integrity client determines which of these three categories the program falls into. In addition, it considers the following factors:

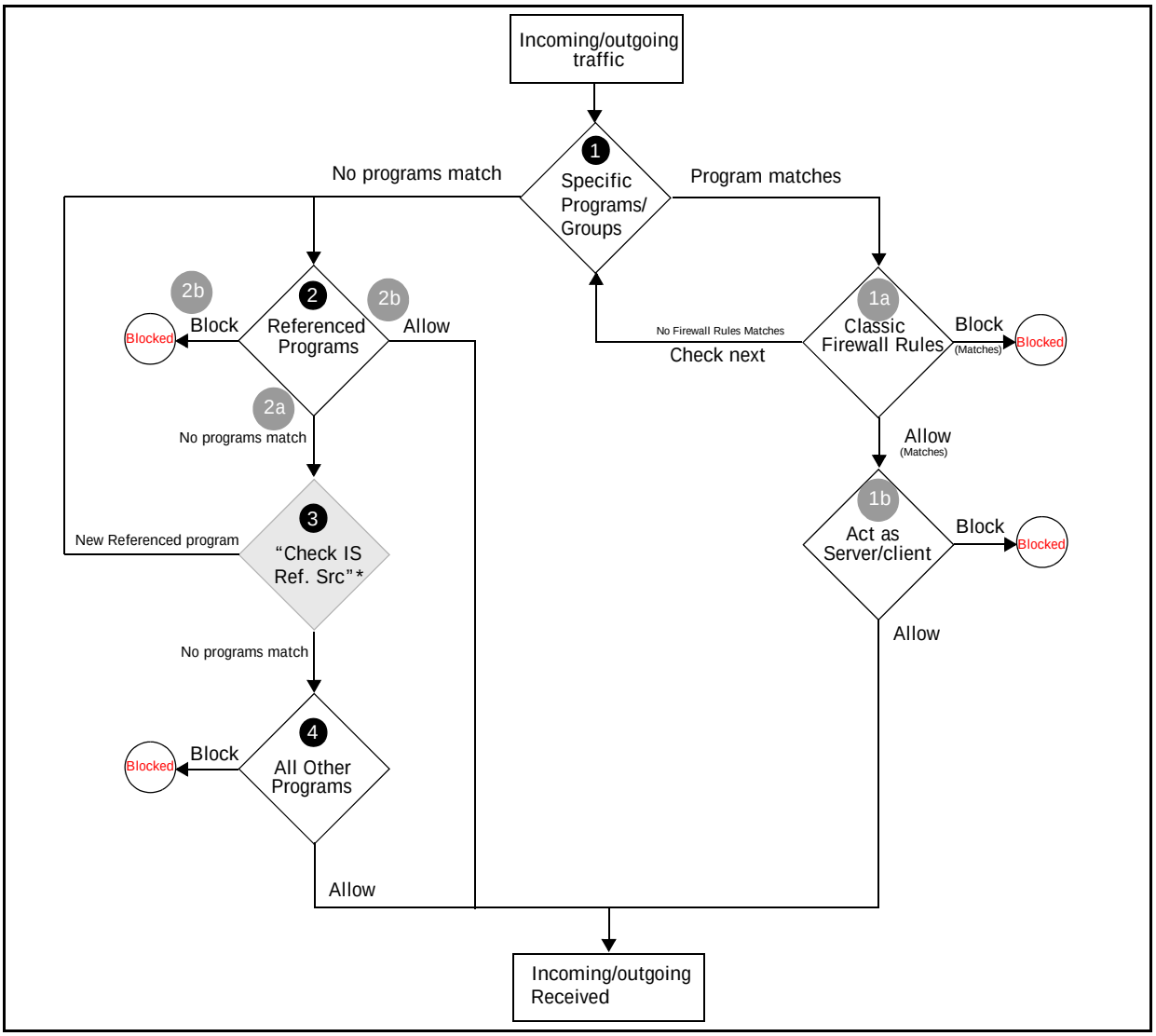
- What Zone (**Trusted**, **Internet**, or **Blocked**) is the program trying to communicate with?
- Is the program trying to establish a connection ("**act as a client**") or listen for a connection ("**act as a server**")?

Based on the answers to those questions, the client takes one of the following actions:

- **Allows** the program to establish or accept the connection
- **Blocks** the program from establishing or accepting the connection
- **Asks the user** whether to allow or block the program

The chart below illustrates in detail how program rules are enforced.

**Figure 7-1:** Security rule evaluation by program rules




1. If the program matches no specific programs and program group rules, then Referenced programs are checked. Go to step 2.

   If the program matches a rule for a specific program or program group, the rules are evaluated as follows:

   **a.** Classic firewall rules are checked.

   - If the traffic matches a **Block** classic firewall rule, traffic is blocked.
   - If the traffic matches an **Allow** classic firewall rule, or does not match any rule, then the program rule is checked. Go to step b.

When no classic firewall rules are assigned to the specific program or program group, only the conditions in step b are applied to the program activity.

**b.** The program rule for the program or program group is checked:

- If the program rule **Allows** the program to act as a server or client, the traffic is allowed. Referenced and All other programs are not checked.
- If the settings **Block** the program from acting as a server or client, the traffic is blocked. No other conditions are checked.

**2.** Referenced programs are checked.

**a.** If the program is not among the referenced programs in the client database, the server setting "Check Integrity Server reference sources for new programs" is checked.

- If **Ask Integrity Server for Reference Sources** is Enabled, the Integrity client queries the referenced sources on Integrity Advanced Server. Go to step 3.
- If **Ask Integrity Server for Reference Sources** is Disabled, the program rule for All Other Programs is checked. Go to step 4.

**b.** If the program is among the referenced programs in the client database, the program rule for referenced programs is checked.

- If the program rule **Allows** the referenced program to act as a server or client, then the traffic is allowed.
- If the program rule **Blocks** the referenced program from acting as a server or client, then the traffic is blocked.

**3.** Integrity Advanced Server searches for the program in its imported reference programs.

- If the program is in a reference source, Integrity client adds the program to the list of referenced programs in the client database, then checks the program rule for referenced programs. Go to step 2b.
- If the program is **not in the referenced group**, Integrity client applies rules for All Other Programs. Go to step 4.

**4.** The program rule for All Other Programs is checked.

- If the rule **Allows** unknown programs to act as a client or server, then the traffic is allowed.
- If the rule **Blocks** unknown programs from acting as a client or server, then the traffic is blocked.

If you have enabled Program Control, see Understanding the Program Advisor Process for information about security rule evaluation using the Program Advisor service.

# Program Control Tools and Features

Integrity Advanced Server provides a number of tools to make it easy to manage program control on your network. The table below summarizes these tools, and shows you where to find information about each.

| Tool/ Feature | With this tool you can... |
|---|---|
| Program Observation | See what applications are accessing your network, and populate Program Manager. Applications appear in Program Manager only after they have been observed.<br><br>See "Observing Program Activity," on page 87. |
| Program Advisor | Use professional recommendations for program permissions.<br><br>See "Understanding Program Advisor," on page 100. |
| Program Manager | Use Program Manager to:<br><br>■ **Set global program permissions** - Set access permissions for programs that apply to your entire organization. See "Setting Global Program Permissions," on page 92.<br><br>Note: If you have licensed Program Advisor, you use Program Advisor to set your global program permissions. See "Program Advisor," on page 100)<br><br>■ **Group programs** - Categorize your programs by type to simplify setting permissions. See "Adding Programs Manually," on page 90.<br><br>■ **Override Program Advisor settings** - If you choose not to use Program Advisor's recommendations, you can use Program Manager to set your own, custom permissions. See "Overriding Program Advisor Recommendations," on page 107<br><br>■ **Add Programs** - You can add a program that has not yet been observed on your system in order to proactively set permissions. See "Adding Programs Manually," on page 90. |
| Reference Sources | Using the SmartSum utility, scan a clean computer configured with your most frequently used applications, then quickly assign program rules to all the applications on that computer.<br><br>See "Creating Reference Sources," on page 83. |

**Table 7-1:** Program control tools and features

| Tool/ Feature | With this tool you can... |
|---|---|
| Program Rules | Configure network access rules for specific programs and groups, referenced programs, and unknown programs.<br><br>See “Creating Program Rules,” on page 93. |
| Advanced Settings | Enable or disable features such as component control and parent process verification. |
| Changes Frequently | By default, Integrity Advanced Server identifies programs by their MD5 or Smart Checksum. This is the safest method of identification, because it rejects programs that have been altered. In some cases, however, you may want Integrity to recognize a trusted program that changes frequently (for example, a program your company updates regularly in-house). You can designate such a program as one that changes frequently, causing Integrity to identify it by file name rather than by MD5 or Smart Checksum. To do so, go to the Program Details page for the relevant program and select **This program changes frequently**. |

**Table 7-1:** Program control tools and features

# Workflow for Program Control

Use the following phases to implement Program Control.

1. **Gather program information**:

   a. **Create and import reference sources**. Use the SmartSum utility to scan a clean, secure computer that has the standard program that you allow to access your network. See "Creating Reference Sources," on page 83.

   b. **Observe program activity.** Have Integrity clients discover and report programs and that are active on your network. See "Observing Program Activity," on page 87.

   c. **Manually add programs.** If you want to set program permissions for a program that has not yet been observed, you may manually add it to the system. See "Adding Programs Manually," on page 90.

   d. **Manage program information.** Create program groups so that you can easily assign rules to programs with similar properties (for example, all Internet browsers). See "Creating Program Groups," on page 90.

2. **Implement program control settings** using the baseline information by:

   a. **Define global program permissions.** Use global program permissions to set permissions for a program for your entire organization. See "Setting Global Program Permissions," **on page 92**.

   b. **Define program rule data.** Define network locations and protocols you want to allow or block. Use the locations and protocols to create classic firewall rules that perform the action you want to assign to the programs. See "Policies: Classic Firewall Rules," on page 57.

   c. **Create program rules.** Create security program rules that associate the programs and program groups with the classic firewall rule you want to use to control the program activity. See "Creating Program Rules," on page 93.

   d. **Add program rules to policies.** Add the program rules to the appropriate policies. See "Adding Program Rules to a Policy," on page 98.

   e. **Deploy security policies to endpoints**. Assign and deploy security policies to end-users to control programs running on the user's endpoint computer. See "Deploying a policy," on page 161.

# Gathering and Organizing Program Information

The first step in implementing program control is to gather and organize information about the applications in use on your network.

Perform the steps found in the following sections:

1. "Creating Reference Sources," in the following section
2. "Observing Program Activity," on page 87
3. "Adding Programs Manually," on page 90
4. "Creating Program Groups," on page 90

## Creating Reference Sources

A reference source is an XML file that contains MD5 and Smart checksums of the programs on a particular computer in your environment.

You create reference sources by running the SmartSum utility (appscan.exe) on a computer with a tightly-controlled disk image, then importing the file into Integrity Advanced Server.

To quickly create **Allow** program rules for the most common applications and operating system files in use on your network, create a reference source for each disk image used in your environment. Then, in your policies, you can create rules for Referenced Programs that will apply to those applications.

The computer you scan to create a reference sources must be free of all malware. If you are certain that your reference scan is "clean," you can use **Allow** permission when you create program rules for Referenced Programs in your policy.

Follow these steps to create reference sources:

1. "Creating a Reference Source File," on page 84
2. "Importing Reference Scans," on page 85

## Creating a Reference Source File

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

To run SmartSum, use one of the following methods:

- "Running SmartSum from the command line," on page 84
- "Running SmartSum using the SampleScan Batch File," on page 85

### Running SmartSum from the command line

This section explains how to execute SmartSum from the command line.

#### To run SmartSum from the command line:

1. Copy SmartSum, located in the `/usr/local/integrity/webapps/ROOT/bin` directory on the Integrity Advanced Server host, to the root directory (typically `c:\`) of the baseline reference source computer.

   For SmartSum to execute on Window 95, 98 or Me operating systems, you also need to copy unicows.dll, located in the `/usr/local/integrity/webapps/ROOT/bin` directory on the Integrity Advanced Server host, to the root directory (typically `c:\`) of the baseline reference source computer.

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

2. On the protected computer, open a command prompt window (go to **Start** | **Run...**, then type **cmd**).
3. In the command prompt window, go to the root directory by entering "**cd **".

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

4. Type **appscan ** to begin the scan.

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

Your reference source scan file is ready to be imported into Integrity Advanced Server.

### Running SmartSum using the SampleScan Batch File

An alternative to running SmartSum from a command prompt is utilizing the **samplescan.bat** file.

#### To use the SampleScan batch file:

1. Copy SmartSum and SampleScan.bat, located in the /`usr/local/integrity/webapps/ROOT/bin` directory on the Integrity Advanced Server host, to the root directory (typically, `c:\`) of the baseline reference source computer.

   For SmartSum to execute on Window 95, 98 or Me operating systems, you also need to copy unicows.dll, located in the `/usr/local/integrity/webapps/ROOT/bin` directory on the Integrity Advanced Server host, to the root directory (typically, `c:\`) of the baseline reference source computer.

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

2. Open SampleScan.bat in a text editor such as Notepad.

   The last statement in the batch file is a command line string.

3. Configure it according to your preferences using the SmartSum command syntax.

4. Double-click the batch file to run the scan.

   The output will be automatically generated in the same directory in which the batch file and SmartSum reside.

Your reference source scan file is ready to be imported into Integrity Advanced Server.

## Importing Reference Scans

After generating a reference source file, import it into Integrity Advanced Server. You can import any of the pre-configured reference sources for other versions of Windows from the Samples folder in your Integrity installation folder.

#### To import a reference source scan:

1. Go to **Global Policy Settings** | **Reference Sources**.

   The Reference Source Manager page appears with the reference source scans listed.

To replace the reference source file from a previous scan, select the reference source, then click **Edit**.

2. Click **Import.**

   The Import Reference Source page appears.

3. Type a description. It is used to identify the reference source.
4. In file to import, either:
   - Click **Browse**, locate the scan.xml, then click **Open**.
   - Type the full path to your SmartSum output file, including the filename, then click **Open**.
5. Click **Save.**

   The Reference Source Manager page appears with the new reference source file listed.

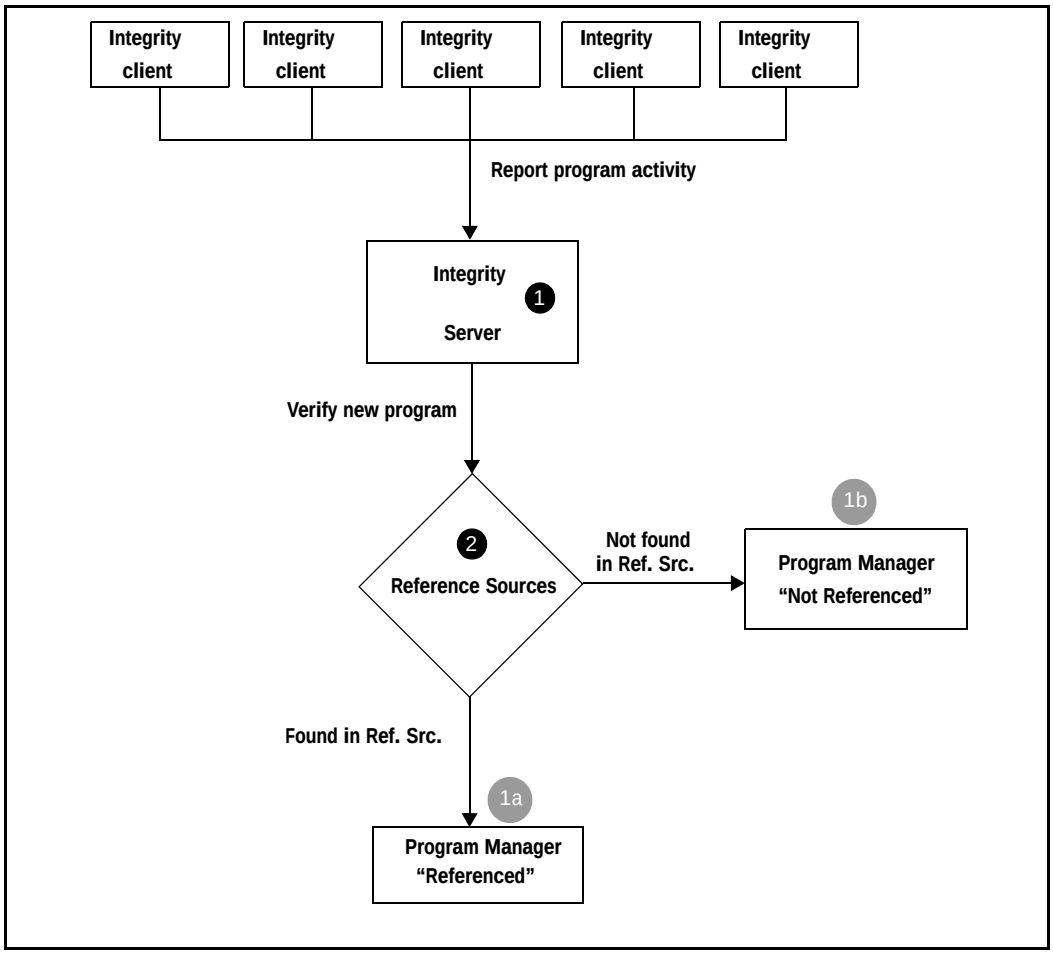
### Setting Rules for Reference Sources

After creating and importing reference sources, you can create policies that include rules for Referenced Programs. For instructions on setting program rules, see "Creating Program Rules," on page 93.

# Observing Program Activity

Use Program Observation to discover the programs that are accessing your network from protected computers. When programs are observed, they appear in the All Programs group in Program Manager. The following diagram shows the process.

**Figure 7-2:** Program observation process




1. Integrity clients record and report all program activity on the protected computer to Integrity Advanced Server.
2. When new program activity is reported, Integrity Advanced Server checks the reference sources to see if the program information is there, then:
   a. If Integrity Advanced Server finds a reference source, it adds the program to the Program Manager in the **All Programs Referenced** group.
   b. If the program is not in reference sources, Integrity Advanced Server adds the new program to the Program Manager in the **All Programs Not Referenced** group.

## Enabling Program Observation

The instructions below explain how to enable Program Observation in an already-assigned policy.

When you are first implementing security with Integrity Advanced Server, the easiest way to enable Program Observation is to deploy a new policy created from the Observation policy template. The Observation template is designed primarily to gather program information.

### To enable Program Observation:

1. Go to **Policies**.

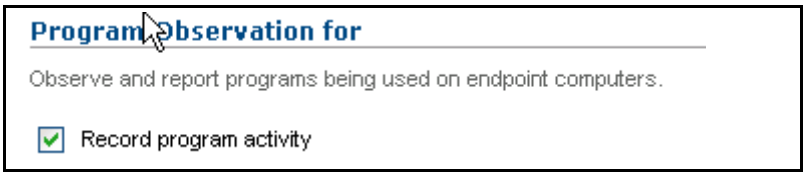
   The Policy Manager page appears. All the policies are listed.

2. Select a policy, click **Edit**.

3. Go to the **Program Rules** tab.

4. Select the **Enable Program Control** check box.


5. Select **Record program activity.** This setting enables program observation.




6. Click **Save**.

   The Version Comments page appears.

7. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

8. Assign and deploy the policy.

After the policy has been deployed, new programs will appear in Program Manager at the end of each observation period. In Program Manager, you can organize these observed programs into groups, in order to manage rules for them easily.

If you are experiencing performance issues, then once you have observed most of the common program activity on your network, turn off Program Observation, then periodically re-enable it to capture new programs. You can also improve performance by increasing the program observation interval. See Setting the Program Observation Interval.

## Setting the Program Observation Interval

Use the program observation interval to control how often program observation information is uploaded to the Integrity Advanced Server.

When you are testing your system with a limited number of users you should set this interval to be about an hour so you can quickly see the results of program observation. However, in full-scale deployments this interval should be set for 24 hours or more to avoid filling up your database.

### To set the program observation interval:

1. Go to **Client Configuration** | **Client Settings**.
2. Click **Edit**.
3. In the **Log Upload Size** section, set the **Program Observation Interval**.
4. Click **Save**.

## Checking the Network for Newly-Observed Programs

When Program Observation is enabled, you can check all relevant endpoint computers for newly-observed programs.

For an overview of newly-observed programs, see “Observing programs,” on page 188.

### To check for newly-observed programs:

1. Go to **Global Policy Settings | Programs**.

   The Program Manager screen is displayed.

2. In the Program Groups area, click the link for the desired program group. (To search the entire network, ensure that **All Programs** is selected.)

   The program list for the selected program group is displayed at right.

3. Above the list of programs, click **Show Filters**.
4. Choose **Observed Within (Days)** from the Field dropdown list, enter a number in the Value field, and click **Apply Filter**.

   The filter returns programs observed for the first time within the specified number of days. When you are done, click **Clear Filter** to return to the complete list of programs.

## Adding Programs Manually

If there is a program that has not been observed on your system that you want to proactively set permissions for, you can add it manually. Adding programs manually and then setting the global permissions to 'block' is especially useful for protecting your system from new malicious programs. For more information about proactively blocking malicious programs, see "Setting Global Program Permissions," on page 92.

### To manually add a program:

1. Go to **Global Policy Settings** | **Programs**.

   The Program Manager page appears.

2. Click **Manually Added**.

3. Click **New**.

4. Enter the information for the program and click **Save**.

   You can now assign global program permissions to the program, or add it to a program group so you can assign program permissions to it on a per-policy basis.

## Creating Program Groups

To enable you to assign rules easily, create customized groups of observed programs, the add observed programs to the group.

You can group programs according to type (for example, Web browsers), according to department (for example, Engineering), or in any other way that matches your enterprise infrastructure.

### To create a program group:

1. Go to **Global Policy Settings** | **Programs**.

   The Program Manager page appears.

2. In Program Groups, click **New**.

   The **New Program Group** page appears.

3. Type a name for the group, then click **Save**.

   The Program Manager page appears with the new group listed under Program Groups.

### To add a program to a program group:

1. Go to **Global Policy Settings** | **Programs**.

   The Program Manager page appears.

2. In the Program Groups list, select the group that contains the program you want to add to the group.

   The program appears in the All Programs list.

If you are adding programs from both the referenced and not referenced groups, you can select All Programs to display every program.

3. In All Programs list, select the program you want to add to the group.
4. In the **Add programs to** drop-down list, select the group.
5. Click **Add**.

   The program information is copied to your group. If the program information changes in the All Programs group, the information in your group is updated.

6. To verify that the program was added, select the program group.

   The programs in the group appear in the All Program list.

To remove a program from the group, in Program Groups, select your group. Then in the All Programs list, select the program and click **Remove**.

You can now configure a program rule for the program group.

# Setting Global Program Permissions

Optionally, you can set program permissions that apply to your entire organization. You might want to set global program permissions to block or terminate known malicious programs.

In order to use global program permissions, you must enable **Ask Integrity Server for Reference Sources** in the Program Rules tab for the policy.

### To set global program permissions:

1. Go to **Global Policy Settings** | **Programs**.

   The Program Manager page appears.

2. Click **Global Permissions**.

3. Click a program name in the list.

   The Global Program Permissions Details page appears.

4. Set the appropriate permissions.

   You can choose to block or allow traffic or ask the user. You can also choose to terminate the application.

Program rules in policies take precedence over global program rules.

# Creating Program Rules

After establishing reference sources and observing the programs on your network, you can begin to create program rules.

## Choosing Program Rules

The rules you apply to programs have an impact on both your level of security and on the level of maintenance effort it will require to make sure that your endpoint users can access needed network or Internet resources.

This section provides a guide to choosing program rules for specific programs and groups, for referenced programs, and for unknown programs.

## Program Rule Types

There are three types of program rules configurable in the Program Rules tab of a policy:

- Rules for **Specific Programs and Program Groups**
- Rules for **Reference Programs**
- Rules for **All Other Programs**

### Rules for all other programs

Use these to set a broad baseline for all unknown programs (that is, those not found in reference programs or in the list of specific programs or program groups).

Rules for unknown programs are crucial to the success of your policy. The more restrictive you are with the “All Other Programs” settings, the more time you must spend adding program rules to the specific program rules section. For detailed information about these settings and their implications, see “Choosing All Other Programs Rules,” on page 95.

### Rules for Referenced Programs

These rules set permissions for programs that are found in any of your reference programs, but for which you have not already created specific rules.

Use these rules to quickly establish permissions for the most commonly trusted applications on your network. If you have created your reference programs from machines you are certain are free of any malware, you can set up Allow permissions, ensuring that those common applications will not be blocked by the Integrity client.

Two other options are available for referenced programs:

- Ask Integrity Server for Reference Sources and Program Advisor recommendations.
- Allow Integrity Flex users to set permissions for unreferenced programs.

See the online help for details on these settings.

### Rules for Specific Programs and Program Groups

These rules block, allow, or terminate a particular program, or a group of programs. Use these rules to create exceptions for specific programs or types of programs (for example, browsers) to the more general rules for reference programs and all other programs. When possible, create rules for groups rather than individual programs, in order to simplify maintenance.

### Advanced Settings

The following advanced settings are available:

- Favor enterprise policy settings when arbitrating program permissions.
- Enforce by checksum only.

See the online help for details on these settings.

## Program Permissions

For each type of rule there are four permissions you must set, summarized in the table below. For each permission, you can choose **Allow** or **Block**. When working with individual programs or program groups, you can also choose to terminate the application.

Each permission carries a different level of risk. The table below lists the permissions from the most risky to allow (acting as a server to the Internet Zone), to the least risky to allow (acting as a client to the Trusted Zone).

| Permission | Description |
|---|---|
| Internet Zone/ Act as Server | Allows/Blocks the application from listening for a connection from a non-trusted server. |
| Internet Zone/ Act as Client | Allows/Blocks the application from connecting to non-trusted computers. |
| Trusted Zone/ Act as Server | Allows/Blocks the application from listening for a connection from a trusted server. |
| Trusted Zone/ Act as Client | Allows/Blocks the application from connecting to servers in the Trusted Zone. |

**Table 7-2:** Program rule permissions

### Internet Zone/Act as a Server

In most cases, you should set this to **Block** for “All Other Programs” and for “Referenced Programs”, allowing only specific programs as exceptions. There are few reasons a standard workstation needs to accept connections.

This is by far the most important of the settings for **All Other Programs**, because these are the connections that present the greatest risk—remote access Trojan horses can listen for connections from hackers; or unauthorized, unpatched FTP and Web servers can be exploited to gain access.

### Internet Zone/Act as a Client

Using the **Block** setting for unknown programs protects you from common threats such as key loggers or remote access Trojan horses. Note, however, that this will block legitimate unknown programs as well—for example, applications with auto-update functions, mail clients, or browsers. To unblock legitimate applications, you must either expand the Trusted Zone to include the computers the application is talking to, or add the application to the specific program rules with permission to act as a client in the Internet Zone.

### Trusted Zone/Act as a Server

This controls whether applications can listen for connections from hosts you have placed in the Trusted Zone. If there are applications in your reference programs that need to accept connections from hosts on your local network, you may want to set this to **Allow** for Referenced Programs. The effectiveness of this setting depends on how well the Trusted Zone is defined—if your Trusted Zone does not contain the clients the application needs to serve, the connection will fail.

### Trusted Zone/Act as a Client

This allows applications to talk out on the Trusted Zone. This is the least risky type of communication to allow.

In most policies, you will want to set this to **Allow** in order to enable the various client applications or processes on your endpoints to communicate with trusted servers on your network.

## Choosing All Other Programs Rules

There are four basic configurations for All Other Programs rules. The table below lists these configurations in descending order, from the least to the most secure. The sections below the table discuss the specifics of these four configurations, presenting the pros and cons of each, and also discusses the impact in the following three areas:

- **Unknown attack protection.** How effectively does the configuration protect against unknown attacks?
- **User restriction.** How much does this restrict what the end user can do?
- **Policy maintenance.** How much time will you have to spend maintaining the policy by adding exceptions and specific program permissions?

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

.

| Configuration | "All Other Programs" Settings | | | |
|---|---|---|---|---|
| | Trusted Zone | | Internet Zone | |
| | Server | Client | Server | Client |
| A) Block Internet Zone servers only | Allow | Allow | Block | Allow |

**Table 7-3:** Possible configurations for program rules

| Configuration | "All Other Programs" Settings | | | |
|---|---|---|---|---|
| | Trusted Zone | | Internet Zone | |
| | Server | Client | Server | Client |
| B) Block all servers | Block | Allow | Block | Allow |
| C) Block All non-trusted communication | Allow | Allow | Block | Block |
| D) Block All | Block | Block | Block | Block |

**Table 7-3:** Possible configurations for program rules

### A) Block Internet Zone servers only

This is the most flexible of the settings, and often the best to start with. Because applications accepting connections pose the greatest risk to the endpoint, this configuration provides effective security. This policy assumes you have defined your Trusted Zone and added any necessary corporate hosts and networks to it. By leveraging the Trusted Zone that has been defined, the few applications that need server rights to operate on the corporate network will have these by default.

.

| Impact area | Level | Description |
|---|---|---|
| Unknown attack protection | Good | Any application that tries to accept a connection from the Internet Zone, that is, an un-trusted host, will be blocked. Applications that accept connections on a desktop present the greatest risk to endpoint computer security. |
| User restriction | Low | Users will be able to run any program that sends traffic to the network. They will also be able to run any programs that accepts a connection from a trusted host. |
| Policy maintenance | Low | Only applications that need to be specifically blocked from sending network traffic, or applications that need to accept connections on the Internet Zone will have to be added to the Specific Programs list. |

### B) Block all servers

If you are not quite sure if your Trusted Zone accurately reflects the level of trust that you want to give all applications, use these settings. This will force you to specifically assign permission to an application needing server rights. Use these settings if you don't want to assume the Trusted Zone is safe to accept connections from.

.

| Impact area | Level | Description |
|---|---|---|
| Unknown attack protection | Very good | Any application that tries to accept a connection will be blocked. Applications that accept connections on a desktop present the greatest risk to endpoint security.<br>Protection/Restriction/Maintenance for “Block all servers.” |
| User restriction | Medium | Users will be able to run any program that send traffic to the network. They will not be able to run any programs that accept connections. |
| Policy maintenance | Medium | Only applications that need to be specifically blocked from sending network traffic will have to be added to the Specific Programs list. |

### C) Block All non-trusted communication

These are appropriate settings when you are comfortable that the Trusted Zone is accurately defined.

.

| Impact area | Level | Description |
|---|---|---|
| Unknown attack protection | Very good | Any application trying to send traffic or accept a connection from the Internet Zone will be blocked.<br>Protection/Restriction/Maintenance for “Block all servers” |
| User restriction | High | Users will be able to run any program that communicates within the Trusted Zone. If a program communicates anywhere on the Internet Zone, it will be blocked. |
| Policy maintenance | Varies | Dependent on Trusted Zone configuration.<br>Provided the Trusted Zone is well defined, the only applications that will need to be added to the "specific programs" listing are applications sending traffic to the Internet. You may also have to periodically review the Trusted Zone to ensure it is accurate |

### D) Block All

The block all option completely prevents applications on the protected computer from communicating with all other computers.

## Adding Program Rules to a Policy

### To add program rules to a policy:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.

   The **Names and Notes** tab appears on the Edit Policy Settings page appears.
3. Select the Program Rules tab.

   The Program Rules page appears.
4. Select the **Enable Program Control** check box if it is cleared.


5. To configure rules for a program or program group:

   a. In Program Rules, click **Add**.

      The Add Program Rules page appears with the program groups from the Program Manager listed.

   b. Select the program or program group you want to add.

      To select a specific program from a group, click the group name, then select the program.

   c. Click **Add**.

      The Program Rules page appears with the programs and groups you added listed.

   d. Complete the settings for the program you added by selecting it and clicking **Edit Settings**. In the Edit Program Rules Settings page, you can:

      - Set program permissions, or specify that the application be terminated.
      - Specify firewall rules for the program.
      - Suppress program alerts and logs. (For information on how this program-specific setting relates to general client settings for program alerts, see “Controlling Program Alerts,” on page 99.)

      When you finish editing the settings, click **Done** to return to the Program Rules tab.

e. Under Referenced Programs and All Other Programs, choose **Allow** or **Block** for each of the four permission types.

All other programs means programs in the Not Referenced groups, moved into the Changes Frequently groups, or those that are new (have never been observed).

6. Click **Save**.

   The Version Comments page appears.

7. In the **Comments** box, type a note that describes the changes to the policy settings, then click **Save**.

   The Policy Manager page appears. The access Zones are now configured.

8. Select the policy, then click **Deploy**.

Endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat; otherwise endpoint users receive the updated policy the next time they log on.

# Controlling Program Alerts

You can configure Integrity Advanced Server to alert endpoint users whenever programs try to (or are asked to) perform restricted functions. To do this, go to the Client Settings tab and select the display option for program alerts. (See "Enabling enforcement rule alerts and logging," on page 129.)

If, on the other hand, you want to keep endpoint users from seeing too many alerts, you have two options:

- Prevent alerts for all programs. To do this, go to the Client Settings tab and deselect the display option for program alerts. (See "Enabling enforcement rule alerts and logging," on page 129.)
- Prevent alerts for *specific* programs. To do this, go to the Client Settings tab and select the display option for program alerts. Then go to the Program Rules tab and select the alert suppression option for each relevant program. (See "Adding Program Rules to a Policy," on page 98, especially step 5.) Settings for individual programs override the general settings in the Client Settings tab.

# Chapter 8
# Program Advisor

## Understanding Program Advisor

Program Advisor is a service provided by Check Point that gives policy recommendations for programs. Use Program Advisor to get professional recommendations from Check Point security professionals about which permissions to assign to common programs. This reduces your workload while improving security and usability. Program Advisor also lets you choose to terminate malicious programs on endpoint computers.

This chapter has the following sections:



## Understanding the Program Advisor Server

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

- Provide program permissions to the Integrity Server

  You can choose to either accept these permission recommendations or override them with custom recommendations of your own.

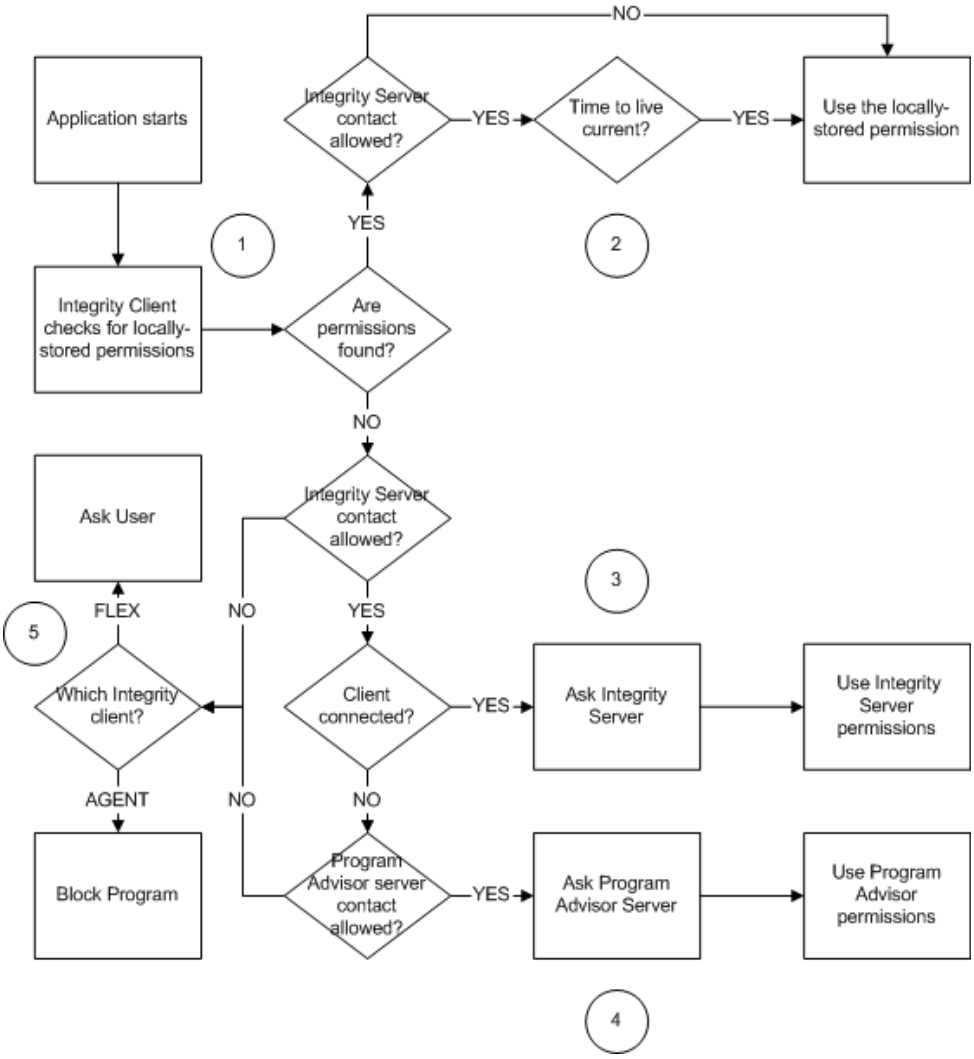
- Provide program permissions to the Integrity client

  You can configure the enterprise policy to allow the Integrity client to access the Program Advisor Server directly if the Integrity client becomes disconnected from the Integrity Advanced Server.

## Understanding the Program Advisor Process

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

## Integrity client Program Advisor process diagram




The following steps describe the Integrity client Program Advisor process:

**1.** The Integrity client checks for locally-stored permissions for the program.

The Integrity client has two sets of locally-stored permissions: those set by the endpoint user, and those set by the enterprise policy.

- If the Integrity client finds locally-stored permissions for the program and you have not set the policy to allow the Integrity client to contact the Integrity Server, the Integrity Client uses the locally-stored permissions.
- If the Integrity client finds locally-stored permissions for the program, and you have set the policy to allow the Integrity client to contact the Integrity Advanced Server, it checks the time-to-live date.

- If the Integrity client does not find locally-stored permissions for the program and you have set the policy to allow the Integrity client to contact the Integrity Advanced Server, it will attempt to contact the Integrity Server to check permission settings.

2. The Integrity client checks the program permission time-to-live date.

   If the client finds locally-stored permissions, and the policy is set to allow the Integrity client to ask the Integrity Server, it checks the time-to-live.

   - If the time-to-live has not expired, the Integrity client uses the locally-stored permissions
   - If the time-to-live has expired, the Integrity client will attempt to contact the Integrity Server to check for new permission settings.

3. The Integrity client asks the Integrity Advanced Server.

   If the Integrity client does not find locally-stored permissions, or the permission time-to-live has expired, and you have set the policy to allow the client to ask the Integrity Server, the Integrity client contacts the Integrity Server to obtain program permissions. See the "Integrity Advanced Server Program Advisor process diagram," on page 103 for more information about this process.

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

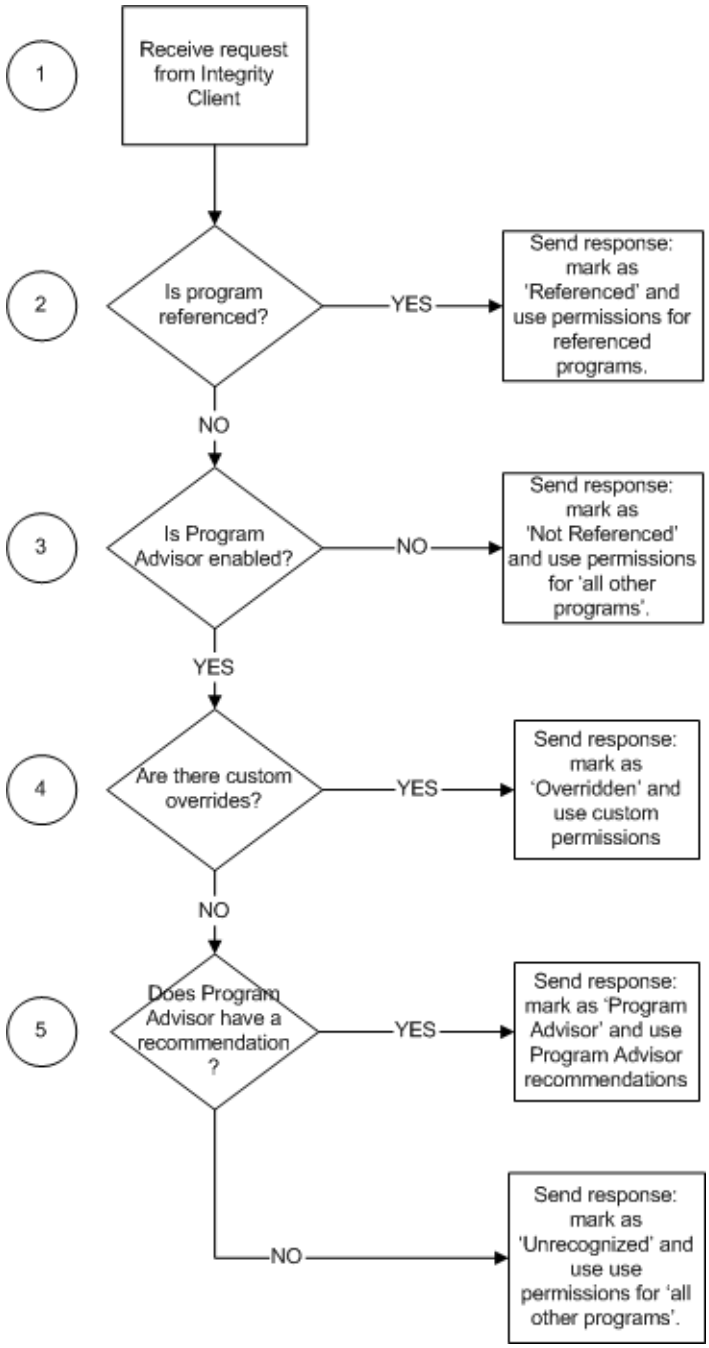
4. The Integrity client asks Program Advisor server.

   If the Integrity client does not find locally-stored permissions, or the permission time-to-live has expired, and the Integrity client is disconnected from the Integrity Server, and you have set the policy to allow the Integrity client to ask the Program Advisor server, it attempts to contact the Program Advisor directly to obtain program permissions.

5. The Integrity client performs client-specific actions.

   - If your endpoints are using Integrity Flex and you have set the policy to not allow the Integrity client access to the Integrity Advanced Server or to not allow access to the Program Advisor Server, the Integrity client will ask the user whether or not to allow access.
   - If your endpoints are using Integrity Agent and you have set the policy to not allow the Integrity client access to the Integrity Advanced Server or to not allow access to the the Program Advisor Server, the Integrity client will block access to and from the program.

## Integrity Advanced Server Program Advisor process diagram




The Integrity server receives program permission requests from the Integrity client. In conjunction with the Program Advisor server, it determines what permissions should be applied to the program, and how it should be displayed in the Program Manager page of the Integrity Advanced Server Administrator Console.

**1.** Integrity Advanced Server receives the request from the Integrity client.

2. Integrity Advanced Server checks for a matching reference source.

   If the program has a matching reference source, the Integrity Advanced Server sends a response to the Integrity client, instructing it to mark the program as 'Referenced' in the Program Manager page. The Integrity client applies the permissions you have set for referenced programs in the deployed enterprise policy. See "Rules for Referenced Programs," on page 93 for more information about setting permissions for referenced programs.

3. Integrity Advanced Server checks if Program Advisor is enabled.

   If Program Advisor is not enabled, the Integrity Advanced Server sends a response to the Integrity client, instructing it to mark the program as 'Not Referenced' in the Program Manager page. The Integrity client applies the permissions you have set for 'all other programs' in the deployed enterprise policy. See "Rules for all other programs," on page 93 for more information about setting permissions for all other programs.

4. Integrity Advanced Server checks for custom overrides.

   You can set Integrity Advanced Server to override Program Advisor's recommendations with your own, custom permission set. If you have set custom overrides for this program, the Integrity Advanced Server sends a response to the Integrity client, instructing it to mark the program as 'Overridden' in the Program Manager page. The Integrity client applies the custom permissions you specified.

5. Integrity Advanced Server checks for Program Advisor recommendations.

   Integrity Advanced Server either contacts the Program Advisor server, or accesses a cached copy of the Program Advisor's previous recommendations. Program advisor recommendations stored on the Integrity Advanced Server include a time-to-live stamp. If the time-to-live period has expired for the program, the Integrity Server must contact the Program Advisor Server to check for new permissions.

   - If Program Advisor has a recommendation for this program, Integrity Advanced Server sends the recommended permissions to the Integrity client. The Integrity client applies the Program Advisor permissions.
   - If Program Advisor does not have a recommendation for this program, Integrity Advanced Server sends a response to the Integrity client, instructing it to mark the program as 'Unrecognized' in the Program Manager page. The Integrity client applies the permissions you have set for 'all other programs'. See "Rules for all other programs," on page 93 for more information about setting permissions for all other programs.

# Using Program Advisor

Perform the following steps to use Program Advisor effectively.

### Implementing Program Advisor:

1. Enable Program Advisor.

   See "Enabling Program Advisor," on page 105.

2. Configure Integrity Advanced Server to work with a proxy server. (Optional. Do this only if your environment includes a proxy server for Internet access.)

   See "Using Program Advisor with a Proxy Server," on page 106.

3. Allow the Integrity client to access the Integrity Advanced Server.

   See "Enabling the Integrity Client to Ask Integrity Server," on page 106.

4. View Program Advisor recommendations.

   See "Viewing Program Advisor Recommendations," on page 107.

5. Implement any overrides (optional).

   See "Overriding Program Advisor Recommendations," on page 107.

6. Manage unknown programs.

   See "Managing Unrecognized Programs," on page 107.

## Enabling Program Advisor

To use Program Advisor in your policies, you must first enable it.

For Program Advisor to work correctly, Integrity Advanced Server must have Internet access so that it can connect to the Program Advisor Server (on ports 80 and 443) and retrieve the latest program information. You must ensure that your firewall allows this traffic. If your environment includes a proxy server for Internet access, perform the configuration steps in "Using Program Advisor with a Proxy Server," on page 106, before continuing with the steps in this section.

### Enabling Program Advisor

1. Go to **System Configuration** | **Program Advisor**.

   The Edit Program Advisor page opens.

2. Click **Edit**.

3. Select **Enable Program Advisor** and enter your **License Key**.

When your license expires, Integrity Advanced Server ceases to respond to program permission requests from Integrity clients. Custom overrides also cease to function, including termination. Locally-stored permissions will remain valid until their time-to-live expires.

4. If you want Program Advisor to terminate the processes for malicious programs, select **Allow Program Advisor to terminate malicious applications**.
5. If you want endpoints to receive Program Advisor recommendations when they cannot contact the Integrity Advanced Server, select **Allow clients to ask Program Advisor directly when the Integrity Server is unavailable**.

If you choose this option, endpoints will receive only the Program Advisor recommendations when disconnected from Integrity Advanced Server. They will not receive any permission overrides you have set until they become connected to Integrity Advanced Server again and either restart the program or receive a new policy.

6. Click **Save**.

# Using Program Advisor with a Proxy Server

If you plan to use Program Advisor in an environment that includes a proxy server for Internet access, perform the configuration steps in "Using Integrity with a proxy server," on page 22 of the *Integrity Advanced Server Installation Guide*.

# Enabling the Integrity Client to Ask Integrity Server

To allow the Integrity client to contact Integrity Advanced Server to obtain program permissions, you must set this option in the policy.

If you do not enable this option, the Integrity clients will not be able to contact Integrity Server or the Program Advisor server and will not receive the full benefit of the Program Advisor service.

### To enable the ask Integrity Advanced Server functionality:

1. Go to **Policies**.

   The Policy Manager page opens.
2. Select your policy and then click **Edit**.

   The Edit Policy page appears.
3. Click the Program Rules tab.
4. Select **Ask Integrity Server for Reference Sources and Program Advisor recommendations**.
5. Click **Save**.

If you want the endpoint computer to receive Program Advisor recommendations directly when it is not in contact with the Integrity Advanced Server, you must choose **Allow clients to ask Program Advisor directly when the Integrity Server is unavailable** in the Edit Program Advisor page. See "Enabling Program Advisor," on page 105.

When using program advisor, do not block incoming traffic to http://<your server IP>/ask/1/ or outgoing traffic to https://cm2.zonelabs.com. Also, do not block traffic to http://pa2.zonelabs.com.

## Viewing Program Advisor Recommendations

You can view all the program permission recommendations that Program Advisor provides in the Program Manager page.

### To view the Program Advisor recommendations:

➪ Go to **Global Policy Settings** | **Programs**.

The Program Manager page opens.

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

Program Advisor does not display recommendations for programs until they are observed on the endpoint computer. If there is a long delay between an Integrity client asking Program Advisor about a program and the log upload containing the observation for that program and if there is also a Program Advisor recommendation for that program, the program recommendations may appear incomplete.

## Overriding Program Advisor Recommendations

If you find you do not agree with a Program advisor recommendation, you can override it with your own custom setting.

### To override Program Advisor recommendations:

1. In the Program Manager page, click the Product Name.

   The Policy Advisor Program Details page opens.

2. Choose the custom settings you want.

   You can override the individual permissions for each Connection Type and Zone with your own settings, or choose to terminate the whole application.

3. Click **Save**.

   When you choose to override a Program Advisor recommendation for a program, a * symbol appears by that program name in the Program Manager page.

## Managing Unrecognized Programs

Once you have deployed a policy and used program observation to detect programs on endpoints, you should periodically check for unrecognized programs. Unrecognized programs are programs that are not referenced, and not governed by either Program

Advisor or a Program Group. You should add these programs to groups so you can assign permissions to them more efficiently.

### To manage unrecognized programs:

1. Go to **Global Policy Settings** | **Programs**.

   The Program Manager page opens.

2. Expand **All Programs**.

3. Click **Unrecognized**.

4. Choose the programs and add them to your program groups as appropriate.

   See "Observing Program Activity," on page 87 and "Adding Programs Manually," on page 90 for more information on observing and grouping programs.

# Chapter 9
# Policies: Restricting Non-Secure Endpoints

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

It is recommended to start out by using rules that observe or warn users (instead of restricting them) so as to avoid interrupting them while you test the rules. Later, you may decide to reconfigure some rules to restrict non-compliant users. Before deploying policies with restriction rules, make sure users have the remediation resources necessary for compliance. If desired, you can configure Integrity Advanced Server to apply remediation resources automatically.

To control program activity on the protected computer, use program rules. (See Chapter 7, “Policies: Program Control.” for instructions.)

# Understanding enforcement rules

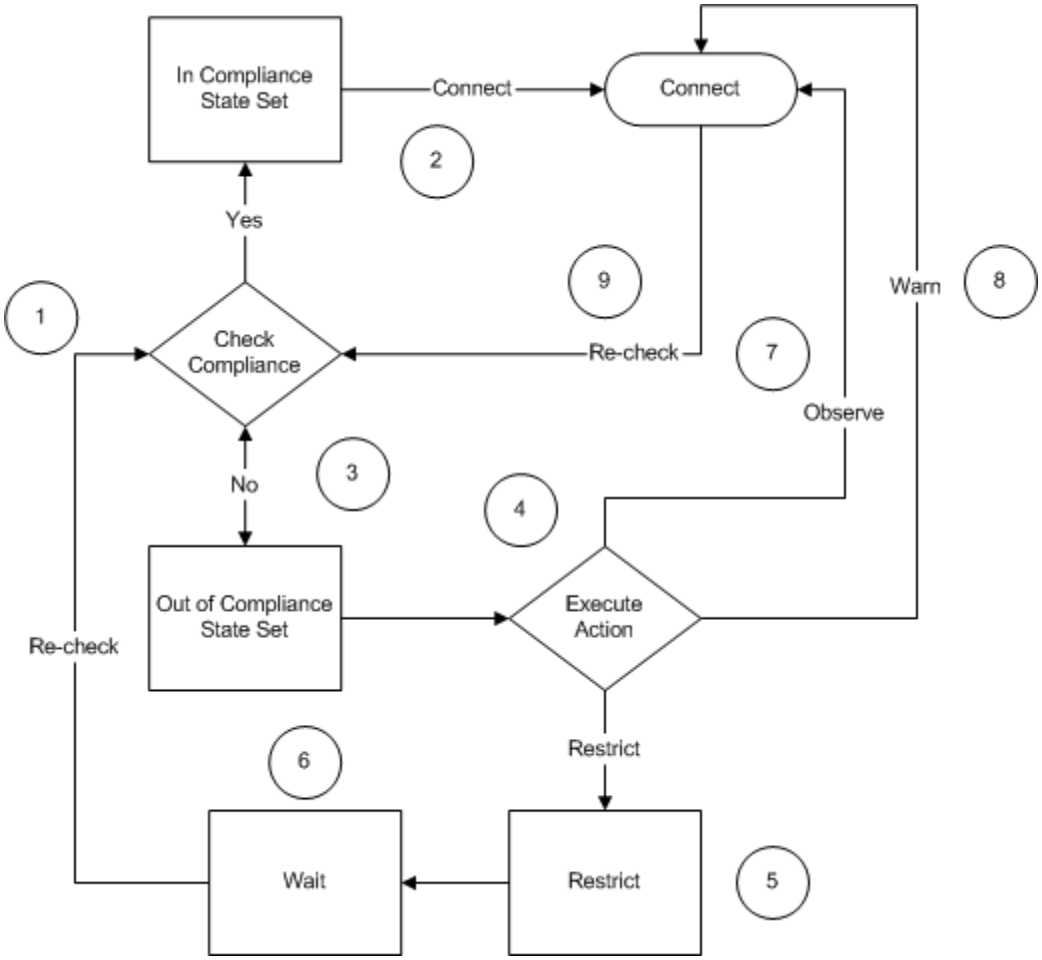
Enforcement rules determine whether the Integrity client can establish and maintain a session with Integrity Advanced Server and your internal network. The Integrity client periodically checks the protected computer for the enforcement rule conditions you set.

Integrity Advanced Server allows you to create the following types of enforcement rules to secure the protected computer:

- General enforcement rules that require or prohibit specific file or program configurations. For example, if you create a rule requiring a specific registry key on Windows NT computers, users establishing a session from a Windows NT computer must have that registry key. Users logging in from Windows NT computers that do not have the registry key are then treated as being out of compliance with the rule.
- Anti-virus provider rules that require a specific anti-virus program, version, and configuration on the endpoint. For example, if you configured a rule requiring McAfee VirusScan Version 4.2 or higher, users logging in from computers that do not have this software are then treated as being out of compliance with the rule.
- Client rules that require an Integrity client on the endpoint computer. For example, if you create a rule requiring Integrity Agent version 6.0, users must have that version of Integrity Agent. Users that do not have Integrity Agent, or which have the wrong version are then treated as being out of compliance with the rule.
- Rule groups that require compliance with a single rule in the group. With a rule group, the computer must be in compliance with at least one of the rules in the group. For example, if you configure a group with rules that require McAfee VirusScan, Symantec Norton AntiVirus, or Trend Micro PC-cillin, then as long as the protected computer complies with one of those rules the user is treated as being compliant with the rule.

## How enforcement rules work

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




1. Integrity client checks the protected computer against all enforcement rules in the assigned security policy, including anti-virus provider rules and groups. The protected computer is found to be either in or out of compliance with the rules.
2. If the protected computer complies with all enforcement rules, the Integrity client sets the state to "In Compliance" and the connection can proceed.
3. If the protected computer is in violation of one or more enforcement rules, the Integrity client sets the state to "Out of Compliance."
4. After the protected computer has been out of compliance for the number of heartbeats you specified, the Integrity client executes the action specified in the

enforcement rule. You can set the Integrity client to observe, warn, or restrict computers that are out of compliance.

5. If you have set the enforcement rule to 'Restrict,' the protected computer will be restricted according to the restriction rules you created for the enforcement rule. The Integrity client will set the state to 'Restricted.' For more information about restriction rules and their impact on the user, see "What a restricted user experiences," on page 112.

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

7. If you set the enforcement rule to 'Observe,' the computer is allowed to connect and the event is logged. For more information about using the observe feature to minimize support requirements while maintaining security see "Using rules that observe or warn," on page 117.

8. If you set the enforcement rule to 'Warn,' the computer is allowed to connect, the event is logged, and the user sees an alert that describes the security violation and provides a link to remediation information. For more information about how to provide your users with the information they need to resolve their own security violations, see "Providing remediation resources for users," on page 115.

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

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

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

# What a restricted user experiences

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

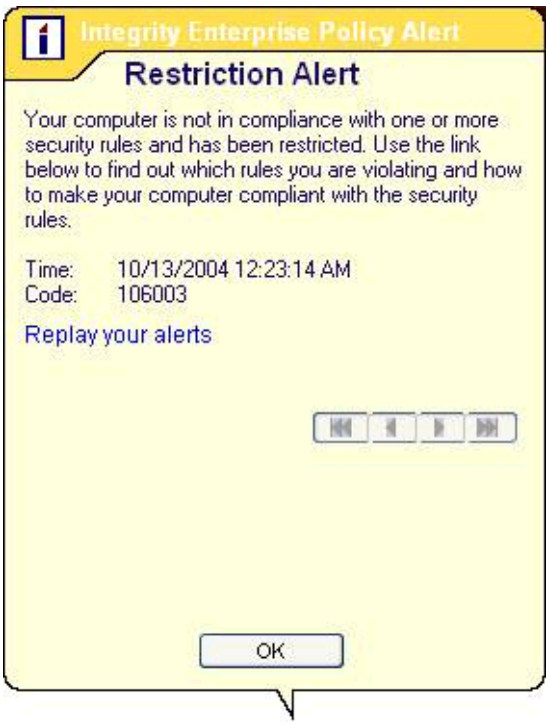
1. Integrity client executes the rule action. The user session is affected as follows:

   - Observed users can access the protected network. Observed users receive no alert.
   - Warned users receive an alert, but can still access the protected network. If you have configured a remediation resource for the rule, Integrity includes the resources (for example, a link or an executable file) in the alert message.

- Restricted users can access only the part of your network you specify using the restriction rules. Generally, you will restrict users to just the sandbox server, where they can get remediation information. If you have configured a remediation resource for the rule, IAS includes the resource (for example, a link or an executable file) in the alert message. If you have configured it to do so, IAS applies the resource automatically.

Warning and restriction alerts include:

- Default or optional customized text explaining the rule action
- The rule name
- Any additional customized text you defined in the policy (optional)
- A help link that opens the sandbox page you created for that enforcement rule




2. If the user clicks the help link, one of the following sandbox pages appears:
   - **REQUIRE** appears when users are not compliant with an enforcement rule that requires a specific program, registry keys/values, or files/properties.
   - **PROHIBIT** appears when users are not compliant with an enforcement rule that prohibits a specific program, registry keys/values, or files/properties.
   - **AV_COMPLIANCE** appears when users are not compliant with an anti-virus provider rule.
   - **GROUP** appears when users are not compliant with at least one of the rules in a group.

3. When the user becomes compliant, Integrity client no longer restricts the session, and the user can access the protected network.

# Minimizing support requirements

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

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

- "Providing remediation resources for users," on page 115
- "Using rules that observe or warn," on page 117

## Providing remediation resources for users

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

- In the enforcement rule, you can specify a remediation resource that users can download and install themselves. For restricted users, you have the option of configuring IAS to run remediation resources automatically.
- In the enforcement sandbox pages (REQUIRE, PROHIBIT, AV_COMPLIANCE, and GROUP).

### To configure remediation resources:

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

| Resource | Description | Configuration Instructions |
|---|---|---|
| Specific details | Provide the specific conditions of the rule. | In an enforcement or anti-virus provider rule, enter custom text that clearly describes the rule conditions with which the user may not be compliant.<br><br>This text displays in the Alert and on the sandbox page. |

| Resource | Description | Configuration Instructions |
|---|---|---|
| Links | Include links to external sites where the user can download the necessary programs or files. | For links on the sandbox page to programs or files needed when a user is out of compliance with a specific rule, include the URL in the enforcement or anti-virus provider rule.<br><br>For links that appear on the sandbox page regardless of the specific rule, set up the link on the relevant enforcement sandbox page. |
| Executable Files | Configure IAS to remediate restricted endpoints by automatically running the necessary executable file. | Configure automatic remediation when setting up the enforcement rule or anti-virus rule. The Integrity client can access the remedial file either directly or through an external URL. |
| Steps | Explain how to install and configure required resources. | On the sandbox page, provide detailed instructions that are specific to all enforcement rules. |
| Technical Support | Technical support contact phone number and/or e-mail addresses for your company. | Include this information in all sandbox pages. |

3. Configure custom text and URLs in enforcement and anti-virus provider rules. (See step 7 in "Creating a new enforcement rule," on page 119.)
4. Configure sandbox pages with specific information related to your rules.
   a. Go to **Client Configuration** | **Sandbox Pages.**
   b. From **Language**, select the language of the page you want to configure.

You must select and modify the sandbox page for each language.

   c. From **Sandbox Pages**, select the page you want to edit.
   d. Modify the **What happened** and **What should I do** areas with specific information for your rules.
   e. Click **Save**.

Non-compliant users now have specific resources and information to help them become compliant.

# Using rules that observe or warn

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

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

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

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

Configure warn rules for software that users are responsible for installing and maintaining themselves.

After deploying a policy with an observe or warn rule, use the Enforcement report in the Reports module of Integrity Advanced Server to track the number of users affected by the rule. By tracking which users are non-compliant and the frequency of non-compliance, and by seeing how long it takes users to come into compliance, you can gauge the effectiveness of your policy and remediation resources.

To log enforcement related events, configure the Client Alerts and Logging on the Client Settings tab of the security policy. (See “Enabling enforcement rule alerts and logging,” on page 129.)

When you are satisfied that your rule and resources will enhance security without unduly increasing your support burden, change the action indicator in the rule from Observe or Warn to Restrict and redeploy the policy. Note that, for rules that restrict, you can configure IAS to apply remediation resources automatically.

### To set the enforcement action for a rule:

➔ In the Rule Action area of the enforcement rule, choose one of the following:

- **Observe clients that don’t comply**
- **Warn clients that don’t comply**
- **Restrict clients that don’t comply**

# Managing enforcement rules

Use the Enforcement Manager to create rules that can be used in security policies to:

- Require or prohibit specific conditions, such as files, programs, or Windows Registry keys and values, on the protected computer
- Require specific anti-virus programs and definition files on the protected computer
- Require a specific type and version of Integrity Client on the protected computer

## Enforcement rule workflow

1. Set up an enforcement rule for each set of conditions you want to enforce in the Enforcement Rules Manager, including setting up the alert message text.

   See "Creating a new enforcement rule," on page 119.

2. Customize the following sandbox pages:
   - **AV_COMPLIANCE** for anti-virus rules
   - **PROHIBIT** for enforcement rules that prohibit programs, files, and/or keys
   - **REQUIRE** for enforcement rules that require programs, files, and/or keys
   - **GROUP** for enforcement/anti-virus rule groups that require one program
3. Assign the enforcement rules to a security policy.

   See "Adding and grouping enforcement rules," on page 127.

4. Deploy the policy and assign it to endpoint users.

   See Chapter 14, "Delivering Policies and Policy Packages to Clients."

# Creating a new enforcement rule


- "Creating a client enforcement rule," on page 124


## Creating a program, file, or key enforcement rule

This section explains how to create rules that require or prohibit programs, a specific file, or registry key entry on an protected computer. It also explains how to set the Integrity client action (observe, warn, or restrict) if the protected computer is out of compliance with the rule. You can specify a remediation resource that users can download and install themselves. For restricted users, you have the option of configuring IAS to run remediation resources automatically.

### To create a enforcement rule:

1. Go to **Policy Objects** | **Enforcement Rules.**

   The Enforcement Rule Manager page appears.

2. Click **New** and select **Enforcement Rule**.

   The New Enforcement Rule page appears.

3. In **Rule name**, type a name to identify the rule.

   The name is used to identify the rule in a security policy in the Policy Manager.

4. From the **Operating systems** drop-down list, choose the protected computer operating system to which this rule applies.

5. Set the rule conditions:

   - Select **Check for registry key or value**, to require or prohibit a specific key value.
   - Select **Check for file and properties**, to require or prohibit a specific file and set the conditions.

6. Select the rule actions:

   a. For **Type of check**, select:

   - **Require these conditions** to require the presence of the registry key or file and properties rule conditions set in step 5 on the protected computer.

     If the conditions are not met, the action you select in step b is taken.

   - **Prohibit these conditions** to prohibit the presence of the registry key or file and properties rule conditions set in step 5.

     If the conditions are met, the action you select in step b is taken.

   b. For **Action**, select:

   - **Observe clients that don't comply** to allow the user session, but notes the compliance violation.

- **Warn clients that don't comply** to alert the user that the computer is out of compliance, allow the user session, and log the compliance violation.
- **Restrict clients that don't comply** to restrict non-compliant users according to your restriction firewall rules.

If you choose to restrict or warn, you should configure the custom text for this enforcement rule and provide a remediation resource. If you choose to restrict, and are not using a supported gateway, you must configure restriction firewall rules for the policies that include this rule, or your users will not be restricted. You must save and deploy the policy for the enforcement rule to take effect.

7. Under Remediation, set the custom text and remediation options. For rules that restrict, you can configure IAS to remediate the endpoint automatically.

   a. Set up custom text that you want to appear in the alert message and on the sandbox page for each language.

The alert appears only if the client alert and logging settings are configured to display enforcement rules on the Client Settings tab of the security policy.

The custom text appears in the alert and on the sandbox page when the protected computer is out of compliance with the rule. Use custom text to help users understand why they are out of compliance and how to become compliant.

The following is an example of custom text in a rule that prohibits a program:

XYZ program is installed on your computer. You must remove this program to regain full access to the network.

   b. Set the remediation options.

      Use the remediation options to help users become compliant. You can provide a remediation resource either by uploading a file or by providing a URL to the resource. For rules that restrict, you can configure IAS to remediate the endpoint automatically. Automatic remediation requires you to specify an executable file as the resource. You can also choose not to provide remediation.

8. Click **Save**.

   The new enforcement rule is created. The Enforcement Rule Manager page appears.

To assign this rule to an endpoint user, add it to a security policy as described in "Using enforcement rules in a security policy," on page 127.

## Anti-virus provider rules

This section explains how to create a rule requiring endpoints to run a specific anti-virus program. If the endpoint becomes non-compliant, Integrity client can restrict

the user session, warn the user without restricting, or observe the violation without restricting. You can specify a remediation resource that users can download and install themselves. For restricted users, you have the option of configuring IAS to run remediation resources automatically.

When creating an anti-virus provider rule, you can enter anti-virus engine and DAT file information manually. However, manual configuration requires frequent maintenance to keep up with software and DAT file updates. You can automate your updates by specifying a single computer (called an anti-virus reference client) to provide software and DAT file information to Integrity Advanced Server. When you update the DAT file or anti-virus engine on the reference client, Integrity Advanced Server updates its anti-virus provider rules accordingly.

To create anti-virus provider rules manually, see "Creating an anti-virus enforcement rule," on page 122.

To create anti-virus enforcement rules based on a reference client:

1. Set up an endpoint computer (the reference client) with the desired anti-virus software engine and DAT file.
2. Configure Integrity Advanced Server to use the anti-virus reference client. (For details, see "Configuring Integrity to use an anti-virus reference client," on page 121.)
3. Assign a policy with an anti-virus enforcement rule to the reference client.

   This lets the reference client report anti-virus engine and DAT file information to Integrity Advanced Server.
4. Create a new anti-virus enforcement rule that uses information from the reference client. (For details, see "Creating an anti-virus enforcement rule," on page 122.)

You can also create an anti-virus program rule for a provider that is not pre-configured on Integrity Advanced Server by following the instructions in "Creating a program, file, or key enforcement rule," on page 119.

### Configuring Integrity to use an anti-virus reference client

Follow the instructions in this section only if you want to use a reference client as the basis of your anti-virus enforcement rule. To configure an anti-virus enforcement rule without using a reference client, see "Creating an anti-virus enforcement rule," on page 122.

### To specify an anti-virus reference client:

1. Make sure the intended reference client has the latest anti-virus engine version and DAT file, and that it is connected to Integrity Advanced Server.
2. Go to **System Configuration** | **Reference Clients**.

   The Anti-Virus Reference Clients page contains entries for all supported providers, whether or not reference clients are configured. Integrity Advanced Server does not display anti-virus software and DAT file details for a given provider until you configure a reference client.

3. Select a provider from the list and click **Configure**.

   The Anti-Virus Reference Client Configuration page appears.

4. Specify the reference client in one of the following ways:

   - To identify the client by IP address, select **IP Address** and type the address in the adjacent field. You must use a static IP address that is dedicated to the reference client.
   - To identify the client by custom user ID (CUID), select **CUID** and enter the path in the adjacent field, or click **Browse** to search for the CUID.

5. Click **Save**.

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

### Creating an anti-virus enforcement rule

Perform the steps below to create an anti-virus enforcement rule for a supported provider.

### To create an anti-virus enforcement rule:

1. Go to **Policy Objects** | **Enforcement Rules.**

   The Enforcement Rule Manager page appears.

2. Click **New** and select **Anti-virus Rule**.

   The New Anti-Virus Provider Rule page appears.

3. Select the desired provider from the Provider dropdown list.

4. Set the rule conditions:

   a. To enforce anti-virus settings from an anti-virus reference client, select **Keep clients in sync with the reference client**. (This option is available only if you have already set up an anti-virus reference client.)

   a. To require a minimum version of the software, select **Minimum engine version** and type the version number.

   b. To require the endpoint to run the anti-virus program, select **This program must always be running**.

   c. Select one of the following DAT enforcement settings:

      - To require a minimum version number, select **Minimum DAT file version** and type the version number.
      - To require a file downloaded on or after a particular date, select **Oldest DAT file time stamp**, then set the date and time.

- To enforce a maximum DAT file age, select **Maximum DAT file age** and type the number of days.

You may encounter time zone issues when using Symantec Antivirus and enforcing by DAT time. Enforce by version for greater accuracy.

5. For the rule action, select one of the following:
   - **Observe clients that don't comply**—allows a non-compliant user to connect, but notes the compliance violation.
   - **Warn clients that don't comply**—alerts the user that the computer is out of compliance, allows the user to connect, and logs the compliance violation.
   - **Restrict clients that don't comply**—restricts non-compliant users according to your restriction firewall rules.

If you choose to restrict or warn, you should configure the custom text for this enforcement rule and provide a remediation resource. If you choose to restrict, and are not using a supported gateway, you must configure restriction firewall rules for the policies you use this rule in, or your users will not be restricted. You must save and deploy the policy for the enforcement rule to take effect.

6. Under Remediation, set the custom text and remediation options. For rules that restrict, you can configure IAS to remediate the endpoint automatically.
   a. Set up custom text that you want to appear in the alert message and on the sandbox page for each language.

The alert appears only if the client alert and logging settings are configured to display enforcement rules on the Client Settings tab of the security policy.

The custom text appears in the alert and on the sandbox page when the protected computer is out of compliance with the rule. Use custom text to help users understand why they are out of compliance and how to become compliant.

The following is an example of custom text in an anti-virus provider rule:

"Anti-virus_program_x" is not running on your computer. You must have a current version of this program installed and running to regain full access to the network.

   b. Set the remediation options.

   Use the remediation options to help users become compliant. You can provide a remediation resource either by uploading a file or by providing a URL to the resource. For rules that restrict, you can configure IAS to remediate the endpoint automatically. Automatic remediation requires you to specify an executable file as the resource. You can also choose not to provide remediation.

7. Click **Save**.

   The new anti-virus rule is created. The Enforcement Rule Manager page appears.

To assign this rule to an endpoint user, add it to a security policy as described in "Using enforcement rules in a security policy," on page 127.

## Creating a client enforcement rule

Use client enforcement rules to require users to have a particular type and version of Integrity client on the endpoint computer.

### To create a client enforcement rule:

1. Go to **Policy Objects** | **Enforcement Rules.**

   The Enforcement Rule Manager page appears.

2. Click **New** and select **Client Rule**.

   The New Client Rule page appears.

3. Enter the **Rule Name**.

4. Choose the **Operating System** this client rule should apply to.

5. Enter the **Rule Conditions** for the rule:

   a. Choose the client type to enforce for, Integrity Agent or Integrity Flex.

   b. Enter the minimum version for this client.

6. For the **Rule Action**, select one of the following:

   - **Observe clients that don't comply**—allows a non-compliant user to connect, but notes the compliance violation.
   - **Warn clients that don't comply**—alerts the user that the computer is out of compliance, allows the user to connect, and logs the compliance violation.
   - **Restrict clients that don't comply**—restricts non-compliant users according to your restriction firewall rules.

If you choose to restrict or warn, you should configure the custom text for this enforcement rule and provide an upgrade resource. If you choose to restrict, and you are not using a supported gateway, you must configure restriction firewall rules for the policies you use this rule in, or your users will not be restricted. You must save and deploy the policy for the enforcement rule to take effect.

7. Under Remediation, set the custom text and upgrade options. For rules that restrict, you can configure IAS to upgrade the client automatically when an endpoint goes out of compliance.

   a. Enter the custom text that you want to appear in the alert message and on the sandbox page for each language.

The alert appears only if the client alert and logging settings are set to display enforcement rules. See the Client Settings tab of the security policy to set the options.

The custom text displays in the alert and on the sandbox page when the protected computer is out of compliance with the rule. If you specified client languages upon setup, you will be able to choose the language for this alert.

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

Integrity Agent v. 6.0 is not running on your computer. You must have a current version of this program installed and running to regain full access to the network.

**b.** Set the upgrade resource.

You must specify an upgrade resource. For rules that restrict, you can configure IAS to upgrade the client automatically when an endpoint goes out of compliance.

**8.** Click **Save**.

The new client rule is created. The Enforcement Rule Manager page appears.

To assign this rule to an endpoint user, add it to a security policy as described in "Using enforcement rules in a security policy," on page 127.

# Editing an enforcement rule

The process of editing rules is similar to creating a new one (see "Creating a program, file, or key enforcement rule," on page 119, "Anti-virus provider rules," on page 120, or "Creating a client enforcement rule," on page 124, for detailed instructions). When you edit a rule used by a security policy, the enforcement, anti-virus, or client rule definition is also modified in the security policy. The modify settings are applied to the security rule the next time the policy is deployed.

# Deleting enforcement rules

Deleting an enforcement, anti-virus, or client rule completely removes the rule from Integrity Advanced Server. These rules are also removed from security policies at the time that you delete them. The change to the security policy is applied the next time the policy is deployed.

### To delete rules:

**1.** Go to **Policy Objects** | **Enforcement Rules.**

The Enforcement Rule Manager page appears.

**2.** Select rules, then click **Delete**.

A confirmation message appears.

3. Click **Yes**.

The rule is deleted from the system and no longer appears in the enforcement rules list. The enforcement rule is removed from existing policies the next time you deploy it.

# Using enforcement rules in a security policy

This section explains how to manage enforcement rules in a security policy.

Assign enforcement rules to prohibit or require specific programs, files, and/or registry keys on the endpoint point computer and determine the action taken when those conditions are met.

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

1. "Adding and grouping enforcement rules," on page 127
2. "Configuring compliance check settings," on page 129
3. "Adding restriction firewall rules to your policy," on page 129
4. "Enabling enforcement rule alerts and logging," on page 129
5. "Configuring the heartbeat interval (optional)," on page 130
6. "Saving the security policy," on page 130

## Adding and grouping enforcement rules

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

### Adding enforcement and anti-virus provider rules

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

**To add rules to a policy:**

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.

   The Edit Policy page appears.
3. Select the Enforcement Settings tab.
4. Under Enforcement Rules, click **Add**.

   The Add Enforcement Rules page appears.
5. Select the rules you want, then click **Add**.

   The Enforcement Settings tab appears with the enforcement rules in the policy.

   If you use restrict or warn enforcement or anti-virus rules, you should configure the Enforcement Alert for this rule and provide remediation resources. If you use a restrict enforcement or anti-virus rule, you should configure Compliance Check

Settings and Restriction Firewall Rules for this policy. You must save and deploy the policy for the enforcement or anti-virus rule to take effect.You can also optionally group enforcement and anti-virus rules.

## Grouping enforcement and anti-virus provider rules

After you add enforcement rules (including anti-virus provider rules) to a policy, you can create enforcement rule groups. When rules are grouped, the protected computer must be compliant with at least one rule in the group.

- The rule action for the entire group supersedes the individual rule actions.
- Automatic remediation is disabled for rules in a group. IAS still provides the remediation resource in the sandbox, but the user has to apply the resource manually. If a rule in the group is used individually in a different policy, automatic remediation still works for the rule in that policy.

### To group enforcement rules:

1. In the Enforcement Settings tab, under Enforcement Rules, select the rules you want to group.
2. Click **Group**.

   The rules you selected are combined into one row and a group title box appears.
3. In the group title box, type a name for the group.
4. Choose the action for the enforcement rule group:
   - **Restrict** - Restricts noncompliant users according to your restriction firewall rules
   - **Observe** - Allows noncompliant users access, and logs the violation
   - **Warn** - Alerts the user that their computer is not compliant, allows the user to access the network, and logs the violation
5. Click **Save** to save the new group.

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

For enforcement rules that restrict, configure compliance check settings and restriction firewall rules for this policy.

You must save and deploy the policy for the rule group to take effect.

## Configuring compliance check settings

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

### To configure compliance check settings:

➔ Set the **Number of non-compliant heartbeats before restriction**.

You must save and deploy the policy for the new compliance check settings to take effect.

## Adding restriction firewall rules to your policy

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

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

1. In the Enforcement Settings tab, under Restriction Firewall Rules, click **Add**.
2. Select the firewall rules you want to use and click **Add**.

   If you need to create a new firewall rule, you can do so by clicking **New Firewall Rule**.
3. Use the up and down arrows to rank the restriction firewall rules.

   Rules are enforced according to their rank.

You must save and deploy the policy for the restriction firewall rules to take effect.

## Enabling enforcement rule alerts and logging

This section explains how to configure Integrity client to display the enforcement rule's custom alert on the protected computer.

If the protected computer is running Integrity Agent in invisible mode, the alerts do not appear even if these settings are configured. However, setting display enforcement alerts directs an alert to the Integrity Advanced Server callback logs.

### To set preferences for alerts and logging:

1. Open a policy and go to the Client Settings tab.

2. Scroll down to Client Alerts and Logs.
3. In the **Enforcement Alerts** row, select:
   - **Display** to display an alert when the user is out of compliance with an enforcement rule.
   - **Log** to have the Integrity client record non-compliant events and report it to Integrity Advanced Server.

   Note that, if you enable display and logging for program alerts, you can override these settings for individual programs by choosing the suppression option for those programs in the Program Rules tab. (For information on suppressing alerts and logs for specific programs, see "Adding Program Rules to a Policy," on page 98, especially step 5. For general information about controlling program alerts, see "Controlling Program Alerts," on page 99.)
4. Optionally, under Custom Messaging, type the custom message and link text that should appear in alerts.

Follow the instructions in the next section to save or to save and deploy your changes to the policy.

# Configuring the heartbeat interval (optional)

Since compliance check settings are regulated by the number of heartbeats, you may wish to adjust the heartbeat interval.

### To configure the heartbeat interval:

1. Go to **Client Configuration** | **Client Settings**.

   If you have not configured client settings, the View Client Settings page shows the default settings.
2. Click **Edit**.
3. In the **Interval** field, enter the number of seconds you want to have between heartbeats.

Setting an extremely low heartbeat interval can result in performance issues. Setting an extremely high heartbeat interval can result in decreased security and less accurate reporting. Typical heartbeat intervals range between 300 and 1800 seconds.

4. Click **Save**.

# Saving the security policy

In order to complete the process of adding enforcement rules to the security policy, you must save your changes. To send the changes directly to the users, you must save and deploy the policy.

### To save or save & deploy the security policy with enforcement rules:

1. On the Policy Settings page, click **Save**.

   The Version Comments page appears.

2. In **Comments**, type a description of your changes, then click:

   - **Save** to save your changes to the policy without deploying.

     The endpoint users do not get a new version of the policy.

   - **Save and Deploy** to save your changes and send the updated policy to assigned endpoint users.

When the Integrity client gets the policy, it begins enforcing the enforcement and anti-virus rules and logging related events.

# Chapter 10
# Policies: Protecting Against Spyware

Integrity Anti-Spyware protects your network from threats ranging from worms and Trojan horses to adware and keystroke loggers. Integrity Advanced Server regularly receives updated spyware definitions from the SmartDefense Anti-Spyware Service, a central server maintained by Check Point. Administrators use these definitions in specific policies or in global Anti-Spyware settings to enforce regular spyware scans and treatments on endpoints.

The following topics are covered:

# Understanding Integrity Anti-Spyware

Check Point maintains up-to-date spyware definitions with its SmartDefense Anti-Spyware Service, a central server in Check Point's offices. Integrity Advanced Server checks the central server twice a day for updates, and populates the administration console with a list of known spyware programs arranged by category.

You can accept IAS's default treatment and action (notification) settings, or modify the settings by spyware category. For example, you might configure IAS to delete Trojans and then notify end users of the deletion. After configuring treatment options, you can enforce regular Anti-Spyware scans and treatments, and then observe, warn, or restrict endpoints that are not successfully scanned and treated at the appointed time.

Your treatment parameters and enforcement settings become part of the policies you deploy to endpoints. After you deploy a policy containing Anti-Spyware settings, IAS distributes updated spyware definitions to clients on each heartbeat, with clients (optionally) notifying end users of updates.

IAS provides reports showing when endpoints have been scanned and which endpoints have been treated for the various categories of spyware.

# Configuring Anti-Spyware

Integrity Advanced Server enforces Anti-Spyware settings through individual policies. You can configure policy-specific settings, and you can configure global settings that can be incorporated into any number of policies. Note that Integrity only enforces global settings when you incorporate them into a specific policy (by selecting **Use global Anti-Spyware settings** in the policy). If you turn off global settings after incorporating them into a policy, Anti-Spyware is disabled in that policy.

The following configuration topics are covered:



## Turning on Anti-Spyware protection

You must turn on Anti-Spyware protection to have access to the various configuration options. The following topics are covered:



### Global Anti-Spyware settings

**To activate global Anti-Spyware protection:**

1. Go to **Global Policy Settings** | **Anti-Spyware**, and click **Edit**.
2. Select **Turn on Anti-Spyware**.

   The other Anti-Spyware settings are now accessible.

### Policy-level Anti-Spyware settings

**To activate Anti-Spyware protection in a policy:**

1. Go to **Policies**, select the desired policy, click **Edit**, and click the Anti-Spyware tab.
2. Select **Turn on Anti-Spyware**.

   The other Anti-Spyware settings are now accessible.

3. Select **Use global Anti-Spyware settings** or **Use policy level Anti-Spyware settings**, as appropriate. The global option is only available after you have configured global settings.

## Setting up regular Anti-Spyware scans

Integrity Advanced Server scans endpoints for spyware and treats any spyware applications it finds. Note that it does not scan removable media, such as USB drives. This section explains how to specify a scan type and a regular scan time.

When considering your scanning schedule, keep in mind any scanning enforcement settings you might implement. For example, if you enforce scanning on a weekly basis, you should schedule a weekly scan. Clients can initiate Anti-Spyware scans, but it is impractical to rely on end users to meet your enforcement requirements. For information about enforcement settings, see "Enforcing Anti-Spyware scans and treatments," on page 136.

### To configure Anti-Spyware scans:

1. In the Scan Settings section of the Anti-Spyware screen, choose a scan method. The choices are:
   - **Scan common locations**—Looks in locations listed in the Integrity Anti-Spyware DAT file. This method requires the least CPU resources and time, but it is also the least thorough.
   - **Scan entire computer**—Looks in all directories for known spyware file names and sizes. This is the default.
   - **Scan entire computer by checksum**—Calculates checksums of all files on the endpoint and compares these to known spyware checksums listed in the DAT file. This method is the most thorough, but it also requires the most CPU resources and time.
2. Choose a day and an hour for regular Anti-Spyware scans. For example, choose **Mondays** and **6 AM**.
3. To delete tracking cookies, select **Scan and delete tracking cookies**.
4. Click **Save**.

## Modifying spyware treatment settings

Integrity Advanced Server divides spyware into several categories, such as adware, keystroke logger, and remote administration tool (RAT). Default scan settings tell IAS to quarantine all spyware and then notify the endpoint user. You can modify the default treatment settings for any or all spyware categories.

### To modify spyware treatment settings:

1. In the Action column next to the appropriate spyware category, choose the desired end-user notification, if any. Options are:

- **Automatic**—Performs the specified treatment *without* notifying the end user.
- **Notify**—Treats the spyware and then notifies the end user about the treatment. The end user cannot cancel the treatment. (This option works only for Integrity Flex users.)
- **Confirm**—Lets end users specify the treatment. End users can choose **Allow** (to let the spyware application run one time), **Always Allow** (to let the application run at any time), **Quarantine**, or **Delete**. (This option works only for Integrity Flex users.)

2. In the Treatment column next to the appropriate spyware category, choose the desired spyware treatment. Options are **Quarantine**, **Delete**, and **Allow**. (The Quarantine option works only for Integrity Flex users. If you choose Quarantine for an Agent user, the client treats it as Delete.)
3. Click **Save**.

# Allowing a spyware program to run

This section explains how to allow individual spyware programs to run. For instructions on allowing an entire category of spyware (adware, for example), see "Modifying spyware treatment settings," on page 135.

### To allow a specific spyware program:

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

# Enforcing Anti-Spyware scans and treatments

You can configure Integrity Advanced Server to enforce regular Anti-Spyware scans and treatments on endpoint computers. Non-compliant endpoints can be observed, warned, or restricted from the network.

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

When you first implement Anti-Spyware scans, it is recommended to observe or warn non-compliant users (instead of restricting them) so as to avoid interrupting users while you test your rule. Later, you may decide to reconfigure the rule to restrict non-compliant users.

When considering your enforcement settings, consider any regular scans you have scheduled. For details on scheduled scans, see "Setting up regular Anti-Spyware scans," on page 135.

### To enforce Anti-Spyware scans and treatments:

1. In the Enforcement Settings section, select **Enforce Anti-Spyware**.
2. Select a time period from the **Maximum Time Since Last Successful Scan** dropdown list. This is the maximum time allowed between successful scans. Endpoints that are not successfully scanned within this period will be observed, warned, or restricted (as specified in the next step).
3. Choose an enforcement option for endpoints that are not successfully scanned within the specified period. Options are:
   - **Observe clients that don't comply**
   - **Warn clients that don't comply**
   - **Restrict clients that don't comply**
4. Click **Save**.

# Anti-Spyware updates

Check Point maintains up-to-date spyware definitions with its SmartDefense Anti-Spyware Service, a central server in Check Point's offices. Integrity Advanced Server checks for updates periodically and downloads new definitions when they are available. After IAS downloads a spyware update, clients with policies that include Anti-Spyware protection receive the update on the next heartbeat. You do *not* have to redeploy a policy to distribute an update.

By default, Integrity Advanced Server checks for spyware definition updates every twelve hours. You can check for an update manually, if desired. This section describes how to view current Anti-Spyware version information and how to check for updates manually.

If you plan to use Anti-Spyware in an environment that includes a proxy server for Internet access, see "Using Integrity with a proxy server," on page 22 of the *Integrity Advanced Server Installation Guide*.

### To view Anti-Spyware version information:

➔ Go to **System Configuration** | **Version Information**.

Integrity displays the Anti-Spyware engine and DAT version, the time of the last server contact, and the timestamp of the last retrieved update. (If you have installed IAS recently, the timestamp may pre-date the installation time.)

### To check for updates manually:

1. Go to **System Configuration** | **Version Information**.
2. Click **Update Now**.

   Integrity contacts the central Check Point server and downloads an update if one is available. This may take a few minutes.

# Monitoring Anti-Spyware protection

Use Integrity Advanced Server reports to monitor endpoint Anti-Spyware scans and to see which endpoints have been treated for the various categories of spyware. This section covers the following topics:



## Checking for Anti-Spyware scans

You can see when or if your clients have performed Anti-Spyware scans.

### To check for Anti-Spyware scans:

1. Go to **Reports** | **Integrity Monitor**.
2. In the Chart dropdown list, choose **Spyware Scanned Date**.

   The Spyware Scanned Date chart appears, showing the latest endpoint scan dates.
3. To see endpoints with particular scan dates, click the appropriate link in the legend.

## Checking for spyware incidents

You can view a report showing detected spyware and subsequent treatments, arranged by spyware category.

### To check for spyware incidents:

1. Go to **Reports** | **Client Events**.
2. Choose a time span for reporting, select **Anti-Spyware** from the Event Type dropdown list, and click **Apply Filter**.

   The Anti-Spyware Events graph appears, showing the number of detections and treatments by spyware category.
3. To see endpoints affected by a specific category of spyware, click the appropriate category link to the left of the graph.

   The Events Details report for that spyware category appears. For more information about the Event Details report, see the online help for that screen. For more information on reporting in general, see "Monitoring Client Security," on page 178.

# Chapter 11
# Policies: Preventing E-mail Attacks

This chapter explains how to protect endpoint computers from e-mail attacks. Integrity Advanced Server provides protection for both inbound and outbound e-mail. Inbound protection prevents potentially harmful e-mail attachments from affecting the endpoint computer by quarantining them until they are approved. This feature consists of a MailSafe Extensions Manager and policy-specific MailSafe Rules. Outbound protection puts limits on outgoing e-mail to prevent e-mail worms and other malicious code from using the endpoint computer to send messages.

Note that inbound MailSafe protection works with POP3 and IMAP4 protocols, while outbound MailSafe works with SMTP protocol only.

This chapter covers the following topics:

# Inbound E-mail Protection

Mailsafe provides and extra layer of protection on the endpoint computer by identifying and quarantining potentially destructive inbound e-mail attachments.

This section is divided into the following topics:



## Understanding Inbound E-mail Protection

When a user receives e-mail, mailsafe compares the extension of the e-mail attachment to a list of attachment types. MailSafe recognizes:

- Normal e-mail attachment delivery
- Base64-encoded attachments
- Unencoded attachments
- Malformed attachments (such as extra spaces and a variety of other tactics)

### What the User Experiences

When an attachment arrives through a POP3 or IMAP mail client that contains a potentially unsafe attachment, Integrity client displays a pop-up alert and quarantines the attachments by changing the filename extension to zl*, with * representing a number or letter (see the quarantine table on page 141 for specifics).

If a user on a protected computer tries to open e-mail with a quarantined attachment type, Integrity client displays a warning message that tells the user to verify that the attachment is safe before removing it from quarantine. The user is still allowed to open the attachment.

### Extension Quarantine Table

When MailSafe quarantines an e-mail attachment, it renames the attachment's file extension. The following table lists commonly quarantined e-mail attachment file extensions and their corresponding MailSafe quarantine extensions:

| Extension | ZL Ext. | Extension | ZL Ext. |
|---|---|---|---|
| ADE | zl0 | MHT | zm8 |
| ADP | zl1 | MSC | zlj |
| ASX | zlz | MSI | zlk |
| BAS | zl2 | MSP | zll |
| BAT | zl3 | MST | zlm |

| Extension | ZL Ext. | Extension | ZL Ext. |
|---|---|---|---|
| CHM | zl4 | NCH | zm3 |
| CMD | zl5 | PCD | zln |
| COM | zl6 | PIF | zlo |
| CPL | zl7 | PRF | zm4 |
| CRT | zl8 | REG | zlp |
| DBX | zlo | SCF | zm5 |
| EXE | zl9 | SCR | zlq |
| HLP | zla | SCT | zlr |
| HTA | zlb | SHB | zm6 |
| INF | zlc | SHS | zls |
| INS | zld | URL | zlt |
| ISP | zle | VB | z1 |
| JS | z0 | VBE | zlu |
| JSE | zlf | VBS | zlv |
| LNK | zlg | WMS | zm7 |
| MDA | zml | WSC | zlw |
| MDB | zlh | WSF | zlx |
| MDE | zli | WSH | zly |
| MDZ | zm2 | | |

## Limitations of Mailsafe e-mail protection

Mailsafe has the following limitations:

- MailSafe does not quarantine e-mail attachments from Web-based e-mail services (such as Yahoo mail or Hotmail) unless the mail is retrieved though a POP server.
- MailSafe does not replace the functionality of anti-virus scanning, but does run in conjunction with anti-virus software. To ensure the proper use of MailSafe when running an anti-virus program, disable the anti-virus program's e-mail attachment scanning feature.
- MailSafe is not compatible with MS Exchange mail servers.

# Managing MailSafe Extensions

This section explains how to use the MailSafe Extension Manager to create, edit, and delete MailSafe extensions. Integrity Advanced Server comes with an out-of-the-box list of MailSafe Extensions, which you can edit or add to as desired.

This section is divided into the following topics:

- "Create a new MailSafe Extension," in the following section

- "Edit a MailSafe Extension," on page 143
- "Delete a MailSafe Extension," on page 144

After you customize your list of MailSafe extensions, you can add extensions from your list to specific security policies. (For details on adding MailSafe extensions to security policies, see"Using Inbound E-mail Protection in a Security Policy," on page 144.)

## Create a new MailSafe Extension

Integrity Advanced Server comes with an out-of-the-box list of MailSafe Extensions. The instructions in this section explain how to create a new extension to add to the list.

### To create a new MailSafe extension:

1. Go to **Policy Objects** | **File Extensions**.

   The MailSafe Extension Manager page appears.

2. Click **New**.

   The New MailSafe Extension page appears.

3. In the **description** box, type a note that is used to identify the extension.

4. In the **extension** box, type the extension you want to add.

   Do not type a period before the extension.

5. Click **Save**.

   The MailSafe Extension Manager page appears with the new extension listed.

To determine a quarantined file's ZL extension, the endpoint user must look in the Integrity client log (tvDebug.log).

## Edit a MailSafe Extension

You can change the settings of an existing MailSafe Extension. Changing an extension modifies it in all the security policies where that extension appears. However, the policies that use the extension must be re-deployed before updating the endpoint user's policy.

### To modify a MailSafe extension:

1. Go to **Policy Objects** | **File Extensions**.

   The MailSafe Extension Manager page appears.

2. Select an extension, click **Edit**.

   The Edit MailSafe Extension page appears.

3. Enter your changes:
   - Type a description that is used to identify the extension.
   - Type the extension you want to add. Do not type a period before the extension.
4. Click **Save**.

The extension is modified in all policies. Note that the policies that have the extension must be re-deployed to deliver an updated policy to the Integrity clients.

Changing an extension listed in the "Extension Quarantine Table," on page 141 automatically maps the modified extension to the same ZL extension.

## Delete a MailSafe Extension

You can delete a MailSafe Extension from the Integrity Advanced Server system, even extensions that are used in security policies. Deleting an extension automatically removes it from all security policies.

### To delete a MailSafe extension:

1. Go to **Policy Objects** | **File Extensions**.

   The MailSafe Extension Manager page appears.
2. Select an extension, click **Delete**.

The extension is removed from the system. The extension is automatically removed from any security policies that included it. However, those policies must be re-deployed to deliver the changes to Integrity clients.

# Using Inbound E-mail Protection in a Security Policy

This section explains how to use MailSafe extensions and MailSafe rules in security policies. Adding e-mail protection to a security policy allows you to protect the endpoint computer from unsafe e-mail attachments.

## Adding e-mail protection to a security policy

Follow the steps below to add an extension created in the MailSafe Extension Manager to a security policy and to configure outbound protection. The same MailSafe extensions can be assigned to different security policies.

### To add e-mail protection to a policy:

1. Open the Policy Manager by clicking **Policies**.

2. Select a policy, then click **Edit**.
3. Select the MailSafe Rules tab.
4. Click **Add**.

   The Add MailSafe Extension to Policy page appears.
5. Select the extensions and click **Add**.

   The Mailsafe Rules tab appears with the extensions set to quarantine.
6. To leave the extensions in the policy without quarantining, clear the quarantine column.
7. Click **Save**.

   The Version Comments page appears.
8. In the Comments box, type a note that describes your changes to the policy settings.
9. If you want to save your changes without deploying the updated policy, click **Save**.

   If you want to save and deploy your changes at the same time, click **Save and Deploy**. Then click **Yes** to confirm.

   The Policy Manager page appears. The MailSafe Extension Rules are now in the security policy.
10. If you saved your changes without deploying, you can deploy your changes by selecting the updated policy and clicking **Deploy**.

When you deploy the policy, endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat. Otherwise, endpoint users receive the updated policy the next time they log on.

## Enabling and disabling an extension quarantine setting

After adding an extension to a policy, you can temporarily disable quarantining of that extension type without removing its definition from the policy. In the quarantine column:

- **Disabled** (not inspected) extensions are cleared
- **Enabled** (inspected) extensions are selected

### To change an extension's quarantine settings in a policy:

1. Open the Policy Manager by clicking **Policies**.
2. Select a policy, then click **Edit**.
3. Select the MailSafe Rules tab.
4. Select the check box in the quarantine column to:
   - Clear quarantine (disable)

- Select quarantine (enable)

5. Click **Save**.

   The Version Comments page appears.

6. In the Comments box, type a note that describes your changes to the policy settings.

7. If you want to save your changes without deploying the updated policy, click **Save**.

   If you want to save and deploy your changes at the same time, click **Save and Deploy**. Then click **Yes** to confirm.

   The Policy Manager page appears. The revised quarantine settings are now in the security policy.

8. If you saved your changes without deploying, you can deploy your changes by selecting the updated policy and clicking **Deploy**.

When you deploy the policy, endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat. Otherwise, endpoint users receive the updated policy the next time they log on.

## Removing a MailSafe Extension from a Security Policy

Removing an extension from a policy does not delete it from Integrity Advanced Server. The extension is still available in the MailSafe Extension Manager, and can be added to this or another policy at a later time.

### To change an extension's quarantine settings in a policy:

1. Open the Policy Manager by clicking **Policies**.

   The Policy Manager page appears.

2. Select a policy, then click **Edit**.

3. Select the MailSafe Rules tab.

4. Select the extension you want to remove, click **Remove**.

5. Click **Save**.

   The Version Comments page appears.

6. In the Comments box, type a note that describes your changes to the policy settings.

7. If you want to save your changes without deploying the updated policy, click **Save**.

   If you want to save and deploy your changes at the same time, click **Save and Deploy**. Then click **Yes** to confirm.

   The Policy Manager page appears. The MailSafe Extension Rules are now removed from the security policy.

8. If you saved your changes without deploying, you can deploy your changes by selecting the updated policy and clicking **Deploy**.

When you deploy the policy, endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat. Otherwise, endpoint users receive the updated policy the next time they log on.

# Outbound E-mail Protection

With MailSafe, you can prevent endpoint computers from sending suspiciously large numbers of e-mails in short intervals and from sending e-mails to unusually large numbers of recipients.

This section is divided into the following topics:



## Understanding Outbound Protection

MailSafe can prevent the propagation of malicious e-mail by placing limits on outgoing messages. You can limit the number of outgoing messages in a given interval as well as the number of recipients per message. E-mail operations that exceed your specified limits trigger a warning to the endpoint user.

## Configuring Outbound Protection

**To configure Integrity client to alert users to suspicious outbound e-mail activity:**

1. Open the Policy Manager by clicking **Policies**.

   The Policy Manager page appears.

2. Select a policy. Click **Edit**.
3. Select the MailSafe Rules tab and locate the Outbound MailSafe Protection heading near the bottom of the screen.
4. To set a number and frequency of outgoing e-mails that trigger a warning to the endpoint user, select the Warn the user when too many messages... check box. Type the number of e-mail messages and the interval in the appropriate text boxes (or accept the defaults of 50 messages and two seconds).
5. To set a number of e-mail recipients that triggers a warning to the endpoint user, select the Warn the user when the number of recipients... check box. Enter the number of recipients that triggers the warning (or accept the default of 50).
6. Click **Save**.

   The Version Comments page appears.

7. In the Comments box, type a note that describes your changes to the policy settings.

8. If you want to save your changes without deploying the updated policy, click **Save**.

   If you want to save and deploy your changes at the same time, click **Save and Deploy**. Then click **Yes** to confirm.

   The Policy Manager page appears. The new outbound e-mail settings are now in the security policy.

9. If you saved your changes without deploying, you can deploy your changes by selecting the updated policy and clicking **Deploy**.

When you deploy the policy, endpoint users who are logged on and assigned to the policy receive an updated version of the policy at the next heartbeat. Otherwise, endpoint users receive the updated policy the next time they log on.

# Chapter 12
# Policies: Protecting Instant Messaging

Integrity IM Security protects endpoint users from IM-based attacks. With IM Security, you control IM traffic by blocking potentially harmful files, scripts, and links, and by enforcing message encryption.

The following topics are covered:

# IM Security basics

Integrity can control and monitor IM traffic, encrypt instant messages, and protect endpoint computers from IM-based attacks. IM Security works by controlling the network protocol for the IM service, so it works with any IM client for the supported services (listed below).

IM Security is a centrally managed feature. There is no capability for enforcing IM Security in personal policies, and Integrity Flex has no user interface to configure settings for this feature.

Use IM Security with any of the following IM services:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Messenger
- ICQ
- Trillian
- Gaim
- Miranda (except with Yahoo! Messenger protocol)

To use IM Security with any instant messenger service in HTTP mode, you must set up a proxy server for HTTP tunneling. Without HTTP tunneling, you cannot apply IM Security to any IM in HTTP mode. For details, see “Configuring IM Security,” on page 152.

# Configuring IM Security

This section explains how to configure IM Security.

### To configure IM Security:

1. Make sure you have already installed one of the supported IM clients. (For a list of supported clients, see "IM Security basics," on page 151.)
2. In the administration console, go to **Policies**, select a policy, click **Edit**, and select the Messaging Settings tab.
3. If **Enable Instant Messaging Security Rules** is not already selected, select it now.

   The IM Security settings become accessible.
4. Select the desired settings. For example, select **Notify the user of the encryption status of each IM**, and then, in the Yahoo column of the service-specific settings, select **Allow Access**, **Block Scripts**, and **Block Executable Links**.

   For a description of all available settings, see online help or "IM Security settings," on page 153.
5. If you want to use IM Security with an instant messaging service in HTTP mode, do the following:
   - Select **Use proxy address (Host:Port)** and type the proxy server host name and port number. Optionally, click **Advanced** and select the instant messaging services that should use the proxy server. By default, all services are selected.
   - In the IM client interface, configure the client to use a direct connection (instead of a proxy server). For example, configure the Yahoo! Instant Messenger client to use **No proxies**.
6. Click **Save**.

# IM Security settings

Consult the associated online help pages for descriptions of IM Security configuration options.

The administration console organizes IM Security settings into general settings that apply to all IM services and service-specific settings that apply only to the particular service(s) you choose.

The Enable Instant Messaging Security Rules setting controls activation of IM Security for the policy. You must select this check box to activate the feature. If you configure IM Security and then clear this check box, Integrity saves your latest settings so that they remain available for re-activation later.

# Monitoring IM Security events

Integrity tracks IM Security events both by IM protocol type and by event type.This section explains how to view reports of IM Security events. (For general information about Integrity Advanced Server reporting, see Chapter 16, "Monitoring Client Security.")

### To monitor IM Security events:

1. Go to **Reports** | **Client Events**.
2. Choose the time span the report should cover and, in the Event Type dropdown list, select **IM Security by Protocol** or **IM Security by Type**.
3. Click **Apply Filter**.

   The appropriate graph appears.
4. To see event details (by event type or by IM protocol, as appropriate), click on the links in the legend.

   The Event Details report displays the user, group, catalog, policy name, and event timestamp for each event.

For information about finding a general report on an endpoint that has had an IM Security event, see "Finding detailed information about individual endpoints," on page 182.

# Chapter 13
# Gateways and Cooperative Enforcement

## Introduction

This chapter describes the Cooperative Enforcement™ feature of Integrity Advanced Server. This chapter contains the following sections:



## Understanding the Cooperative Enforcement feature

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

- are running an Integrity client.
- have a specific policy.
- comply with the security policy assigned to them.

Using the Cooperative Enforcement feature, you can restrict or terminate the VPN session for any endpoint computer that is out of compliance.

If you are using a Check Point InterSpect™ internal security gateway, you can also have intra-LAN cooperative enforcement. See the *Integrity Advanced Server Gateway Integration Guide* for more information.

## Supported Gateways and Clients

Integrity Advanced Server can perform Cooperative Enforcement protection with the following gateways and clients:

- Check Point Software Technologies VPN-1 SecureClient and Firewall-1 using Secure Configuration Verification (SCV)
- Check Point InterSpect™ internal security gateways
- Cisco VPN 3000 Series Concentrator
- Nortel Contivity VPN switch with TunnelGuard, Firmware version 4.80 or later

If you use an unsupported gateway, Integrity Advanced Server can monitor Integrity client events and the user status, but it will not be able to restrict access at the gateway level. You must use Enforcement rules in conjunction with Restriction Firewall rules to restrict endpoint users. See "Policies: Restricting Non-Secure Endpoints," on page 109.

# Configuring Cooperative Enforcement

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

### To configure Cooperative Enforcement:

1. Add the gateway to your Integrity Advanced Server.

   See "Adding a gateway catalog," on page 11. This step allows the Integrity Advanced Server to communicate with your gateway device.

If you are setting up Cooperative Enforcement with Check Point InterSpect, configure the InterSpect gateway first and Integrity Advanced Server second. This means that, for InterSpect, you must begin with step 4 and then go back to complete steps 1-3.

2. Add groups to the gateway.

   See "Adding groups to custom, IP, and gateway catalogs," on page 17.

   If you are using Check Point Interspect, you should not add groups or assign policies.

3. Assign policies.

   You can assign policies to a group and/or to the gateway itself. See "How policy inheritance works," on page 8.

4. Integrate your gateway with the Integrity Advanced Server.

   For information specific to your gateway type, see the appropriate chapter of the *Integrity Advanced Server Gateway Integration Guide*.

# Chapter 14
# Delivering Policies and Policy Packages to Clients

This chapter describes how to deliver enterprise security policies and policy packages to Integrity protected computers. It includes information about the end-to-end delivery process, policy version management, and both policy and policy package assignment.

# Understanding policy delivery

Integrity Advanced Server enterprise security policy delivery consists of four major steps:

1. **Saving** a policy on Integrity Advanced Server. This process saves a policy on Integrity Advanced Server without making it available to Integrity clients. Saved policies can be the first version, an updated version, or an old version restored through rollback.

   See Chapter 4 Managing Policies, "Creating a new security policy" for detailed instructions on creating policies.

2. **Deploying** a policy to the policy server area of Integrity Advanced Server. This sends the latest version of a policy to an area where it is available for download by Integrity clients.

3. **Assigning** a policy to one or more entities. This is how a policy is associated with a user on the Integrity Advanced Server system.

The steps involved in assigning a policy package are the same as for assigning a policy.

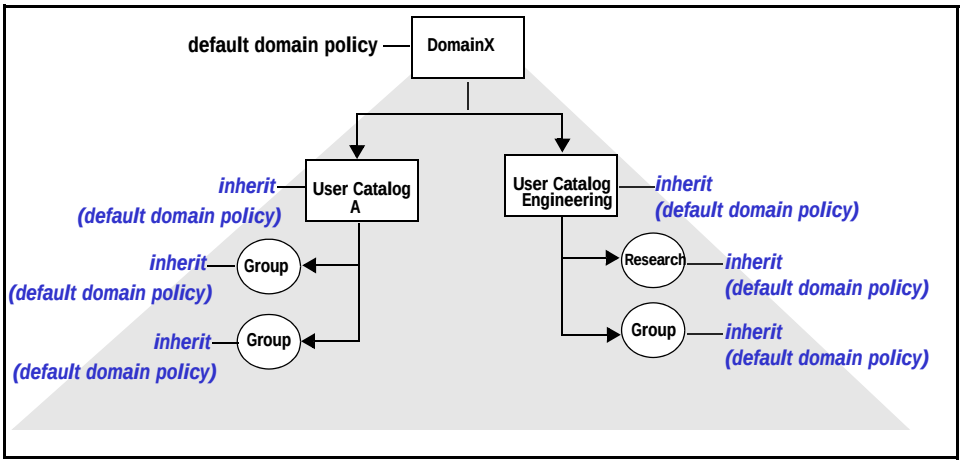
4. **Downloading** a policy from the Integrity Advanced Server policy server by Integrity clients. This is how Integrity clients get the latest version of the policy assigned to the user logging in from the computer where the client is installed.

## About policy inheritance

A policy is always assigned to every entity. Integrity automatically assigns the default policy to newly-created entities. You can then assign policies either directly or through inheritance (from the parent entity).

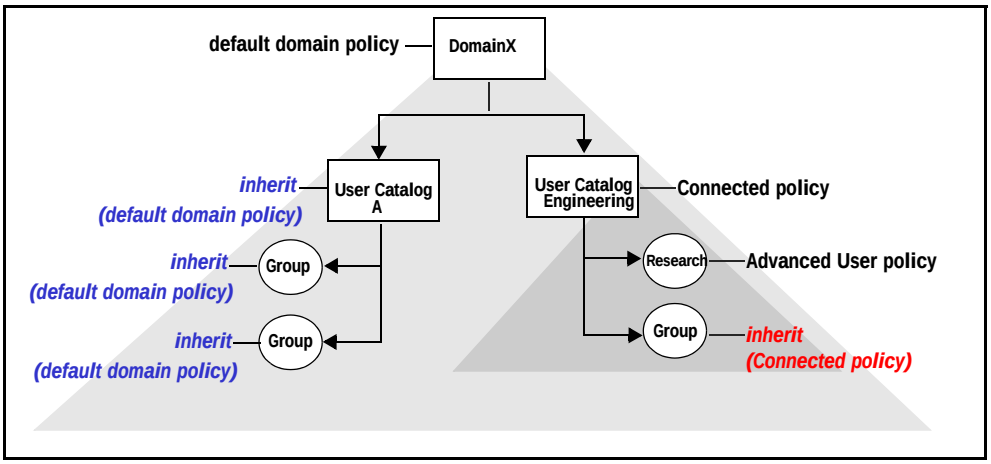
The following two scenarios illustrate policy inheritance:

- **Scenario 1**: The **default policy** is assigned to DomainX and all the entities are set to inherit. (This is the default behavior.)



All the catalogs and groups inherit the default policy.

- **Scenario 2**: The **default policy** is assigned to DomainX, the **Connected policy** is assigned to the Engineering user catalog, an Advanced User Policy is assigned to the Research group (under the Engineering catalog), and all other catalogs and groups are set to inherit.




The Research group users have the Advanced User policy, other Engineering groups inherit the Connected policy, and all other catalogs and groups inherit the default policy.

For instructions on how to assign policies to entities, see "Assignment scenarios," on page 162.

# Managing policy versions

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

When you restore policy settings, the policy has the current definitions from the data managers, such as Classic Firewall Rules Manager and Location Manager. Occasionally, the following conditions may occur when you roll back to an earlier version of a policy:

- The rule or definition was modified in the data manager. In this case, the policy includes the most current settings for rule or definition.
- The rule or definition was deleted from the data manager. In this case, the policy includes that rule or definition. The deleted rule or definition becomes local to the policy; it does not appear in the data manager.

The maximum number of policy versions that Integrity Advanced Server stores depends on the initial configuration of the server. Once the version history reaches the maximum, the earliest copy is removed and the most recent one is saved.

### To roll back a policy to a previous version:

1. Choose **Policies**.

   The Policy Manager page appears.

2. In the list of policies, select a policy, then click **History**.

   The Policy History page displays the version history of the selected policy.

3. View policy settings for the saved version.

   Inspect the policy settings to find the version you want to restore.

   a. Entries in the Date Saved column are hyperlinks to a read-only view of that version's policy settings. Click the hyperlink to view the settings.

   b. When done viewing settings, click **Return to Policy History**.

4. In the version list, select a version, then click **Roll Back**.

   A confirmation message appears.

5. Click **Yes**.

   The Policy Manager page appears with a message indicating the success of the rollback.

After you have rolled back to a previous version, you must deploy the policy to send it to the assigned users. You may want to modify the policy settings before deploying it.

# Deploying a policy

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

### To deploy a policy:

1. Choose **Policies**.

   The Policy Manager page appears.

2. In the list of policies, select the policy to deploy and click **Deploy**.

   A confirmation message appears.

3. Click **Yes**.

   The Policy Manager page appears with a message indicating the success of the deployment. The Last Deployed On field updates with a current time stamp.

After a policy has been deployed, you can assign it to entities. Assigned entities download the policy on the next heartbeat or the next time they log in.

# Assignment scenarios

This section covers common policy administration tasks:

- "Assigning a policy to entities," on page 162
- "Assigning a policy to users (optional)," on page 162
- "Setting the security model," on page 163
- "Setting policy assignment to inherit," on page 163
- "Deleting an assigned policy," on page 164

The steps for assigning a policy package are the same as for assigning a policy.

## Assigning a policy to entities

This section explains how to assign a policy to an entity.

**To assign a policy:**

1. Go to **Entities**.

   The Entity Manager page appears.

2. Select the desired entity and click **Assign Policy**. (If the desired entity does not appear on screen initially, use the Search function to find specific entities, or click on entity and group links to navigate through the hierarchy. If an entity does not have a check box, you do not have permission to access that entity.)

   The Policy Assignment page appears.

3. In the **Select Policy** dropdown list, select the policy to assign. If you select a policy that has not been deployed, the assignment process automatically deploys it.

4. Click **Assign**.

If you assign policies to either users or groups *and also* to IP ranges or subnets, you must decide which policy should be enforced for users belonging to both. See "Setting the security model," on page 163.

## Assigning a policy to users (optional)

Users automatically inherit policies from their parent entities. However, you can assign a different policy directly to one or more users without having to create a new entity just for those users. Use this feature for exceptions to your general security practices.

### To assign a policy to users:

1. Go to **Entities**.

   The Entity Manager page appears.

2. Click on the entity and group links to navigate to the user level. Select the desired user and click **Assign Policy**.

   The Policy Assignment page appears.

3. In the **Select Policy** dropdown list, select the policy to assign. If you selected a policy that has not been deployed, the assignment process automatically deploys it.

4. Click **Assign**.

If you assign policies to either users or groups *and also* to IP ranges or subnets, you must decide which policy should be enforced for users belonging to both. See "Setting the security model," on page 163.

## Setting the security model

A user may be subject to more than one security policy. For example, a user might belong to a group that gets policy x, but have an IP that is assigned policy y. The security model determines policy precedence in such cases.

By default, user and group policies have priority over the IP-based policies, and unknown users and IP addresses receive the default policy.

### To set the security model:

1. Go to **System Configuration** | **Security Model**.

   The Security Model page opens.

2. Select the security model and use the up and down arrow keys to control priority.

   Security models are enforced in the order they appear in the Security Model page. You can also choose to disable or enable a security model.

## Setting policy assignment to inherit

Every entity on Integrity Advanced Server must have a policy assigned to it at all times. (Even new entities are automatically assigned the default policy when they are created.) To remove a direct policy assignment, you must make the entity inherit the policy of its parents.

### To configure policy inheritance:

1. Go to **Entities**.

   The Entity Manager page appears.

2. Select the desired entity and click **Assign Policy**. (If the desired entity does not appear on screen initially, use the Search function to find specific entities, or click on entity and group links to navigate through the hierarchy.)

   The Policy Assignment page appears.

3. In the **Select Policy** dropdown list, select **Inherit from parent**.

4. Click **Assign**.

## Deleting an assigned policy

You cannot delete policies while they are still assigned to entities. To delete a policy, first find all entities to which the policy is assigned, and then assign a different policy to those entities. After changing the policy assignment, remove the old policy. For instructions, see “Deleting a security policy,” on page 50.

# Chapter 15
# Integrity Client Installation Packages

This chapter describes how to create and deliver Integrity client installation packages to protect endpoint computers. This chapter begins with a discussion of what is an Integrity client installation package and how to create one. It continues with sections describing how to deliver a client package to the endpoint. Finally it shows how to auto-update a client package using a client rule.using a client rule.

This chapter only describes the client package administration tasks that are performed using the Integrity Advanced Server Administrator Console. For more information about Integrity clients and how to deploy them to endpoint computers, see the ***Integrity Advanced Server Client Management Guide***.

It is recommended that the Integrity client be the only firewall on the endpoint computer.

# Understanding Integrity client installation packages

A client installation package, at a minimum, consists of an Integrity client installer executable and configuration information. The configuration information is represented in XML format. It can be automatically generated by the client packager or you can manually edit an existing XML configuration file and include it in the client package.

We recommend you use **Client Packager** to automatically generate the XML configuration file. The client packager provides default settings for the connection string that will correctly connect Integrity client to Integrity Advanced Server. The configuration information, combined with the installer settings, provides the connection string to the Integrity Advanced Server from which policies are downloaded and managed. In addition, a client package can also include a personal and/or a disconnected policy.

## The Integrity client executable

Integrity Advanced Server includes a default Integrity client executable for each type of Integrity client: **Integrity Flex** and **Integrity Agent**. Integrity Flex is intended to be deployed to autonomous users with a degree of familiarity with desktop protection functionality. Integrity Flex users would be expected to have the technical knowledge to be responsible for their own firewall configuration. Integrity Flex provides the capability for the user to configure the personal policy settings. Unlike Integrity Flex, Integrity Agent is designed to be configured entirely by an administrator. You should choose which type of Integrity client to deploy based on your enterprise requirements and end user capabilities.

## The configuration information

The configuration information provides the client with the information necessary for it to connect to the Integrity Advanced Server and download the enterprise policy assigned to it. (These configuration settings are stored in the configuration XML file that is contained in the client package.) Other configuration options define the behavior of the Integrity client.

Configuration information (config.xml) for Integrity client can be created in two ways:

- Automatically; using the Integrity Advanced Server **Client Packager**, select configuration settings in the **Use configuration information below** section. The configuration information is automatically generated by the client packager. We recommend this method for creating the configuration information.
- Manually; use the Policy Studio **Export** feature to export a policy to an XML configuration file. Edit the XML configuration file, then use the Client Packager **Use configuration file** radio button to import the XML configuration file.

## XML configuration file

The XML configuration file encapsulates the connection string and all the configuration options for running Integrity client.

See the *Integrity Client Reference Guide* for details on how to work with the XML configuration file and for a full range of parameters you can use to configure the client.

# Disconnected endpoint security

The personal policy defines the Integrity client behavior when the client is disconnected from the enterprise network. Integrity Flex users can change their personal policy settings, however, Integrity Agents users cannot.

A default personal policy exists in the Integrity client. You can add an administrator configured policy to the client package to replace the default personal policy. In this way you can provide a baseline for endpoint security when the client is disconnected.

Alternatively, to create a baseline for endpoint security while disconnected, you can add a disconnected policy to the client package. (The disconnected policy is used when the client cannot access Integrity Advanced Server.)The disconnected policy arbitrates with the personal policy, but cannot be changed by the endpoint user. During arbitration the strictest rule prevails, whether it comes from the disconnected policy or the personal policy. Another advantage of a disconnected policy over a personal policy is that it can be centrally managed by Integrity Advanced Server. A disconnected enterprise policy and a connected enterprise policy can be packaged by the administrator, creating a policy package. This policy package can be centrally managed and distributed to the endpoint even if the initial client package did not include a disconnected policy.

For more information about creating personal and enterprise policies (connected and disconnected), see Chapter 4, "Security policies,".

# Creating an Integrity client package

To create an Integrity client package, you perform the following steps:

1. "Choose a client configuration method and settings," on page 168
2. "Create security policies," on page 168
3. "Create the client package and add client package information," on page 169
4. "Configure the client package," on page 170
5. "Set the client installation parameters," on page 171

## Choose a client configuration method and settings

Prepare for creating a client package by choosing a method to configure the client settings and choose which client configuration settings to implement.

### To prepare for creating a client package:

1. To provide client configuration settings, choose one of the following methods:
   - Create an XML configuration file or edit an existing pre-configured XML configuration file in Integrity Advanced Server's **Policy Studio**. For more information see "The configuration information," on page 166.
   - When creating the client package, type the configuration information directly into the **Use configuration information below** section.
2. Select the client configuration settings most suitable for your enterprise environment. To see a full list of configurable client settings, see the *Integrity Client Reference Guide*.

   Next create the security policies that you want to include in the client package, see "Creating an Integrity client package," on page 168

## Create security policies

You do not need to create any security policies at this point. If you choose not to create a security policy the default enterprise policy is used. However, before creating a client package, you can create the security policies to enforce on the client and/or include in the client installation package. The following is a list of the optional security policies to create:

- **Personal policy**; the personal policy contains Integrity client settings that are used when the enterprise policy is not active.
- **Connected enterprise policy**; when the client first connects to Integrity Advanced Server it downloads the connected enterprise policy assigned to it.
- **Disconnected enterprise policy**; include a disconnected policy in the client package or download it in a policy package (connected and disconnected enterprise policy package).

For more detailed information on the various types of policies and their usage, see Chapter 4, "Security policies,".

Next create the client package and add client package information, see "Create the client package and add client package information," on page 169.

# Create the client package and add client package information

Create a client package and add the client package information. This information identifies the client package and defines the type of Integrity client to include in the package.

### To create a client package and add the client package details:

1. Go to **Client Configuration** | **Client Packages**.

   The Client Packager page appears.

2. Click **New**.

   The New Client Packager page appears.

3. In the **Package Details** section, type the name of the new package in the **Package Name** field.

4. In the **Product Information** section, from the **Client Type** drop-down list, select the type of Integrity client to include in the package.

5. Click **Browse** and navigate to select the client installer file to include in the package.

6. In the **Product Version** field, type the version number for the Integrity client.

It is important to include the full version number in the **Product Version** field. Providing a full version number allows you more refinement when creating an auto-update **Client Rule** for auto-updating the client. There are several ways to find the client version number:

- Note the full version number when downloading the client from the client download Website.
- The Integrity client installer files provided with Integrity Advanced Server includes the version number in the filename.
- In the Integrity client user interface, choose the **Overview** panel, then **Product Info** tab. The client version number displays.
- In Windows Explorer, right click the client file, select **Properties**. Click the **Version** tab and click **Product Version**. The client version number is displayed in the Value field.

7. If the Integrity client is a localized version, then in the **Language** drop-down list, select the language for that localized client.

   Next configure the client package. (See "Configure the client package," on page 170.)

# Configure the client package

Perform one of the following set of steps to configure the client package:

- Configure the client package with an XML configuration file
- Configure the client package using the **Use configuration information below** section.

### To configure the client package with an XML configuration file:

1. In the **Configuration Details** section, select the **Use configuration file** radio button.
2. Click **Browse** and navigate to the XML configuration file to use as the client configuration file.

### To configure the client package manually:

1. In the **Configuration Details** section, select the **Use configuration information below** radio button.

   The **Connection Name**, **Server IP Address**, and **Server Port** fields are automatically filled with the Integrity Advanced Server information to which you are currently connected.

   If you are creating a client package to use with the auto-update feature and you want to use reporting, then you must use the same IP address, server port number, and user ID for the updated client package as you used for the initial client deployment.
2. In the **User ID** field, type a user group if you want to group clients by a custom user ID.
3. Optionally, in the **Single Sign On ID** field, choose the single sign on type.
4. In the **Reconnect Interval** field, keep the default setting or type the number of seconds/minutes to specify the interval at which Integrity client attempts to connect to Integrity Advanced Server. (The reconnect interval is also known as the sleep time between connection attempts.)

   - Values less than 10 are interpreted as minutes
   - Values greater than 10 are interpreted as seconds

   The default value is 180 seconds.

If Integrity Advanced Server is unavailable, Integrity client suspends operation for 3 minutes, at which time the client makes a new attempt to reconnect. Use the **Reconnect Interval** field to shorten the interval between reconnect attempts.

5. In the **Enforce Enterprise Policy** drop-down list, select one of the following options:

   - **Always**; enforces the enterprise policy when the endpoint is either connected to or disconnected from the enterprise network.

Depending on whether a disconnected enterprise policy is used or not, the **Always** setting causes different behaviors.

- If a connected enterprise policy is the only enterprise policy, then this enterprise policy is enforced when connected or disconnected. (The enterprise policy's **Policy Arbitration Rules** settings are ignored. Instead the client packager's **Enforce Enterprise Policy** | **Always** setting takes precedence.)
- If a disconnected enterprise policy exists (whether included in the client package or downloaded from the Integrity Advanced Server), then the disconnected policy is enforced and its own **Policy Arbitration Rules** settings are used

   - **When connected**; enforce the enterprise policy only when connected to the enterprise network.

6. Select the following check boxes if they are relevant to your enterprise:

   - **Launch Client Minimized**; minimizes the client when Windows launches (Integrity Agent only)
   - **System Tray Icon**; shows system tray icon (Integrity Agent only)
   - **System Tray Menu**; allows system tray right-click menu (Integrity Agent only)
   - **Client Shutdown**; allows users to shutdown Integrity client while the enterprise policy is being enforced or not. The enterprise policy can be either a connected or a disconnected enterprise policy, depending on the connection status. (This option is available for both Integrity Flex and Agent clients.)

7. If you want to include a local policy in the client package, then select a policy from the **Add Local Policy** drop-down list.

See "Disconnected endpoint security," on page 167 for more information about including a personal policy in the client package.

8. If you want to include a disconnected enterprise policy in the client package, then select a policy from the **Add Disconnected Policy** drop-down list.

See "Disconnected endpoint security," on page 167 for more information about including a disconnected enterprise policy in the client packager.

# Set the client installation parameters

The client installation parameters define the behavior of the client installation process.

### To set the client installation parameters:

1. In the **License Key** field, type the license key provided to you by Check Point sales.

2. In the **Install Directory**, type the file path where you want Integrity client to be installed on the endpoint machine.

If you leave this field blank, then Integrity client is installed in the following default path: `C:\Program Files\Check Point\Integrity Client`

3. If you want the end user to view the Integrity client installation user interface as the client is installing, clear the **Run Installer without UI** check box.
4. Select one of the following **Install Key** radio buttons.

The install key options control whether or not the end user can uninstall Integrity client and suppress installation notification dialogs.

- **Don't use an install key**; allows the client to be installed without a install key.
- **Use and set an install key**; allows you to set an install key. This install key is required to uninstall the Integrity client. You must provide the install key in the **Install** Key field.
- **Use an install key and change it to a different key on installation**; allows you to update an existing Integrity client with an install key to a new client with a new install key. You must provide the existing install key in the **Install Key** field and the new install key in the **Set Install Key** field.

5. In the **Install Key** field, type one of the following:
   - If you selected the **Use and set an install key** radio button, then type the install key.
   - If you selected the **Use an install key and change it to a different key on installation** radio button, then type the existing Integrity client's install key. You type the new install key in the **Set Install Key** field.
6. In the **Set Install Key** field, type the new install key for the Integrity client that is to replace the Integrity client to be updated.
7. In the **Additional Parameters** field, type additional command line switches or properties and values to further refine the installation behavior.

   For detailed information on the permitted switches and properties, see the *Integrity Client Management Guide*.
8. Optionally, you can choose to install a server certificate with this package.

Make sure you have finished configuring your server before adding a server certificate. If you deploy a package with a server certificate and then change the server or update the server certificate, your endpoint users will be unable to connect.

9. Optionally, you can include a registry file in the package.

   You may want to use registry files to identify the endpoint computers that belong to your organization. See Chapter 9, "Creating a program, file, or key enforcement rule," for more information about requiring registry keys on endpoint computers.

10. Click **Save**.

    The Client Packager page appears with a message indicating the policy package was created successfully.

# Editing an Integrity client package

Use the **Edit Client Package** page when you want to modify the sets of an existing client package. You can edit all the fields of an existing Integrity client package.

### To edit a client package:

1. Go to **Client Configuration** | **Client Packages**.

   The Client Packager page appears.

2. Select the client package to edit, then click **Edit**.

   The New/Edit Client Package page opens.

3. Edit the **Package Detail** section's field.

4. Edit the **Product Information** section's fields:

   - To keep the current Integrity client executable file, select the **Use current installer** radio button.
   - To choose a new Integrity client executable file, select the **Browse for new Installer File** radio button.

5. Edit the **Configuration Details** section's fields:

   - If you want to use the current configuration file, select the **Use current configuration file** radio button.
   - If you want to select a new configuration file, select the **Browse for new configuration file** radio button.
   - If you want to use the current configuration information below or edit the configuration information below, select the **Use configuration information below** radio button.

6. Edit the **Install Parameters** section's fields.

7. Click **Save**.

   The Client Packager page appears with a message indicating the policy package was updated successfully.

# Copying an Integrity client package

You can copy a client installation package to create a new client package with the same settings as the copied client package.

### To copy a client package:

1. Go to **Client Configuration** | **Client Packages**.

   The Client Packager page appears.

2. Click **Duplicate**.

   The New/Edit Client Package page appears.

3. In the **Package Name** field, type the name of the new client installation package.

4. Edit any other fields that you want to change.

5. Click **Save**.

   The Client Packager page appears with a message indicating a copy of the policy package was created successfully.

# Deploying an Integrity client package

There are two ways to deploy a client package. You can export the client package and distribute it to the endpoint user using your own distribution method or you can distribute a link that directs the endpoint user to a sandbox page that includes the client package.


- "Distributing a client package file," on page 176


## Distributing a client package file

### To export a client package:

1. Go to **Client Configuration** | **Client Packages**.

   The Client Packager page appears.

2. Click **Export**.

   The File Download page appears.

3. Click **Save**.

Do not click the **Open** button as the executable will install on the administrator's console machine.

4. Browse to the location where you want to save the client package and click **Save**.

   You can now use which ever distribution method you choose to distribute the Integrity client package to your end point users.

### To distribute a URL to download the client

1. Go to **Client Configuration** | **Client Packages**.

   The Client Packager page appears.

2. Click on the client package name that you wish to distribute.

   The View Client Package page appears.

3. Copy the **Package Download** URL.

4. Distribute the URL to endpoint users using e-mail or your intranet:

   - E-mail the full path of the client package to endpoint users. Users can simply click on the hyperlink provided or copy and paste the URL into a browser address field.
   - Post the download URL to your intranet as a convenient method of software distribution.

Both of the above methods rely on the endpoint user's cooperation. However, once clients are installed, upgrades can be handled seamlessly by way of policy enforcement and auto-update.

# Auto-updating a client package

You can update endpoint clients automatically by creating a client rule and referring to the location of the updated client package. The client rule sets the minimum client version allowed on an endpoint. You can set the remediation options to automatically upgrade the client with the endpoint user's confirmation, or prompt endpoint users to upgrade.

For more information about creating client rules and using auto remediation see "Creating a client enforcement rule," on page 124.

# Chapter 16
# Monitoring Client Security

Integrity Advanced Server provides a variety of reports for monitoring security on your endpoints. Reports show whether your endpoints comply with client and policy requirements, enforcement rules, firewall rules, regular Anti-Spyware scans, and anti-virus software requirements. They also provide information about endpoint security events, such as prohibited program activity and prohibited file transfers over IM or email. If a user is unknown, reports provide user connection information instead of a catalog name. Reports present overviews of general security trends as well as detailed information about individual endpoints.

The following topics are covered:

# Setting log upload parameters

Integrity Advanced Server bases its reports on logs uploaded from clients. Log upload parameters have default values, but you can change the defaults to control how often clients send the logs.

### To set log upload parameters:

1. Go to **Client Configuration** | **Client Settings**.

   If you have not already configured client settings, the defaults are displayed.

2. Click **Edit**.

3. Complete the fields to configure the parameters.

Setting excessively low parameters can result in a loss of performance. Setting excessively high parameters will result in your reports being less up-to-date.

# Getting an overview of your endpoints

Integrity Advanced Server provides graphical overviews of endpoint connectivity, client deployment, policy assignment, Anti-Spyware scan dates, and compliance with enforcement, anti-virus, and client rules. Reports include links to lists of endpoints arranged into relevant categories.

This section explains how to access all endpoint overview reports. It also describes the following specific reports:

- "Client Connectivity report," on page 180
- "Client Version report," on page 181
- "Policy Assignment report," on page 181
- "Anti-Virus Scanned Dates report," on page 181
- "Anti-Virus DAT Update Status report," on page 181

For information about endpoint compliance reports (Current Client Compliance Status, Client Compliance by Rule, and Client Compliance by Policy), see "Tracking enforcement-rule compliance," on page 183. For information about the Spyware Scanned Date report, see "Monitoring Anti-Spyware protection," on page 139.

### To see an endpoint overview report:

1. Go to **Reports** | **Integrity Monitor**.
2. From the Chart dropdown list, choose the desired report.

   The desired report appears.
3. To see a list of endpoints in a particular category, click the appropriate link in the legend. For example, to see a list of disconnected endpoints in the Client Connectivity report, click the Disconnected link in the legend.

   A list of relevant endpoints appears. Filter options at the top of the screen help you search for particular endpoints.
4. Optionally, click on an individual user in the list to see the Endpoint Details report for that user. (For more information about the Endpoint Details report, see "Finding detailed information about individual endpoints," on page 182.)

## Client Connectivity report

The Client Connectivity report gives an up-to-date overview of connected and disconnected clients. Connected clients are organized according to how long they have been connected. The report keeps you up to date on connectivity issues, such as when an unusual number of endpoints are disconnected during working hours.

A client is connected when the endpoint computer is turned on and the user is logged in. It is therefore normal for a majority of endpoints to be disconnected during non-working hours, when most users have turned their computers off.

## Client Version report

The Client Version report shows which client versions are running on your network and which endpoints are running them. Use the report when you have deployed a new client package and want to confirm that endpoints are running the new client.

## Policy Assignment report

The Policy Assignment report shows policies that are assigned to your endpoints. Use the report when you have deployed a new or updated policy and want to confirm that endpoints have received the new assignment.

The Policy Assignment chart's legend may occasionally contain error categories such as "User not resolved" or "Group not resolved," indicating that you have not assigned a policy to all entities, that you have removed a group or catalog without updating the policy assignment, or that there is a problem with the client's connection information.

## Anti-Virus Scanned Dates report

Use the Anti-Virus Scanned Date report to see when your endpoint computers were last scanned. If you find that your endpoints are not being scanned sufficiently often, you may need to use the enforcement feature to require they be scanned.

## Anti-Virus DAT Update Status report

If your users do not have recent virus definition updates, they will not be protected against the most recent viruses. Use the Antivirus DAT Update Status report to see what versions of the virus definitions your users have.

# Finding detailed information about individual endpoints

Integrity Advanced Server maintains an Endpoint Details report for each endpoint computer. The report includes general endpoint information, a list of any enforcement rules the endpoint has violated, a list of any required security providers (such as Anti-virus providers), and a table of statistics on endpoint-specific client events.

You can search for individual Endpoint Details reports by user, IP address, or other criteria, or you can access them through the various Integrity Monitor reports. (For general information about Integrity Monitor reports, see "Getting an overview of your endpoints," on page 180.)

### To see endpoint details:

1. Do one of the following:
   - Go to **Reports** | **Endpoints**.
   - Go to **Reports** | **Integrity Monitor** and choose a report from the Chart dropdown list. To see a lists of relevant endpoints, click on the graph itself, on a link next to the graph, or on a link in the the legend. (Options differ depending on which report you selected.)
2. When the list of endpoints appears, access a particular Endpoint Details report by doing one of the following:
   - Scroll through the list of endpoints and click on a user link.
   - Search for a particular endpoint by entering the desired filter values (user ID, assigned policy, and so on) and clicking **Apply Filter**. Note that, if your filter parameters apply to only one endpoint, IAS displays the report for that endpoint. If your parameters apply to more than one endpoint, IAS displays a table listing all relevant endpoints. Click on a user link in the table to see the report for that endpoint.
3. View the report. Optionally, you can click on links in the report to see the endpoint policy, the Endpoint Compliance History, any enforcement rules the endpoint has violated, and reports on endpoint-specific client events.

# Tracking enforcement-rule compliance

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

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

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

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

This section covers the following topics:



## Viewing current compliance

The Current Client Compliance Status report shows which clients currently comply with your enforcement rules and settings, and which clients do not. Integrity Advanced Server also provides reports that show compliance events organized by rule and by policy.

The Current Client Compliance Status report divides clients into five categories:

- **Compliant**—the endpoint complies with all enforcement rules and settings.
- **Non-Compliant**—the endpoint violates one or more enforcement rules configured to observe the user.
- **Restricted**—the endpoint has violated a rule configured to restrict the user, and the user has subsequently failed to remediate the endpoint in the grace period. (The default grace period is four heartbeats, though you can configure the grace period in the policy.)
- **Terminated**—the endpoint has violated a rule configured to restrict the user, and the user has subsequently failed to remediate the endpoint in the allowed time.

(The default time allowed is six heartbeats after restriction, though you can configure the allowed time in the policy.)

- **Disconnected**—the endpoint is not connected to Integrity Advanced Server. Note that a client is connected when the endpoint computer is turned on and the user is logged in to the network. It is therefore normal for a majority of endpoints to be disconnected during non-working hours, when most users have turned off their computers.

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

### To access the Integrity Monitor compliance reports:

1. Go to **Reports** | **Integrity Monitor**.
2. From the Chart dropdown list, choose one of the compliance reports. Options are **Current Client Compliance Status**, **Client Compliance by Rule**, and **Client Compliance by Policy**. (Descriptions of these reports can be found in the first part of this section.)

   The desired report appears.
3. To see a list of endpoints in a particular category, click the appropriate link in the legend.

   A list of relevant endpoints appears. Filter options at the top of the screen help you search for particular endpoints.
4. Optionally, click on an individual user in the list to see the Endpoint Details report for that user. The Non-Compliance Status section of the Endpoint Details report lists the enforcement rules and settings the endpoint has violated. (For more information about the Endpoint Details report, see "Finding detailed information about individual endpoints," on page 182.)

## Viewing compliance history

Integrity Advanced Server provides two kinds of reports on compliance history: a general history and endpoint-specific histories. After viewing the general report, you can navigate to the compliance histories of individual endpoints.

### To view compliance history:

1. Go to **Reports** | **Client Events**.
2. Choose a time span for the report and select **Compliance Status** from the Event Type dropdown list. Click **Apply Filter**.

   The Compliance graph appears, showing the number of compliance events at various points within the reporting period.

3. Do one of the following:

   - To see a list of all endpoints with compliance events within the reporting period, click directly on the graph.
   - To see a list of endpoints by category, click the appropriate link in the legend.

   A list of relevant endpoints appears. Filter options at the top of the screen help you search for particular endpoints.

4. Optionally, view an individual endpoint's compliance history. To do so:

   a. Click on an individual user in the list.

   b. In the Endpoint Details report that appears, find the General Information section and click on the Compliance State link.

   The Endpoint Compliance History appears, showing compliance status over time and the number of violations.

# Tracking client security events

Security events occur when endpoints violate your security settings (such as firewall rules, program rules, MailSafe rules, and Anti-Spyware scan requirements). When an Integrity client detects a violation, it logs the event and uploads event data to Integrity Advanced Server. IAS presents this data in several Client Events reports organized by event type. In addition, a summary report provides an overview of all client events.

IAS maintains the following Client Events reports:

- **Summary**—provides a summary of all event types.
- **Firewall**—shows violations of classic firewall rules or Zone rules. There are separate reports for inbound and outbound firewall events.
- **Compliance Status**—shows violations of enforcement rules, anti-virus rules, client rules, and Anti-Spyware scan settings.
- **Client Errors**—shows all endpoint events for users. Note that client-rule compliance is monitored in the Compliance Status report.
- **Anti-Spyware**—shows detections and treatments of spyware programs.
- **MailSafe**—shows violations of MailSafe rules. There are separate reports for inbound and outbound firewall events.
- **Malicious Code Protection (MCP)**—shows violations of Malicious Code Protection rules. There are separate reports for inbound and outbound firewall events.
- **IM Security**—shows violations of IM Security enforcement settings. There are separate reports showing events by IM protocol and events by type.
- **Program**—shows events related to program rules.

For each of these event types, IAS provides an overview chart or graph and a legend with links to lists of affected endpoints. For example, the IM Security by Type report consists of a graph showing events and a legend with several links, including one called “Files Received.” That link leads to a list of endpoints that have received files over IM.

The rest of this section explains how to access Client Events reports. For further information about the Anti-Spyware report, see “Monitoring Anti-Spyware protection,” on page 139. For further information about the IM Security report, see “Monitoring IM Security events,” on page 154. For further information about the Compliance Status report and related reports, see “Tracking enforcement-rule compliance,” on page 183.

### To view Client Events reports:

1. Go to **Reports** | **Client Events**.
2. Select a time span and event type for the report, and click **Apply Filter**.

   If you choose Summary for the event type, IAS displays a summary of all client events with links to individual event-type reports. Choosing any other event type causes IAS to show the relevant report immediately.

3. When the event-type report appears, you have two options for finding event details:
   - Click on the graph to see Event Details reports listing endpoints that experienced an event of that type.
   - Click on legend keys to see reports for endpoints in various subcategories.

# Monitoring programs on your network

Use Integrity Advanced Server reports to track program events and to observe programs on your network.

This section covers the following topics:



## Tracking program events

The Program report summarizes program *events* . An event is any action that violates a program rule. This report does *not* summarize all program activity. (For options on finding information about general program activity on your network, see . For information about the Program Observation report, see "Observing programs," on page 188.)

You can view program events by event timestamp (the default), user, group, catalog, or user event count. IAS also provides reports on up to five of the programs associated with the most events.

### To access the Program report:

1. Go to **Reports** | **Client Events**.
2. Choose a time span for the report and select **Program** from the Event Type dropdown list. Click **Apply Filter**.

   The Program report appears, showing recent program events and (at the bottom of the screen) a list of the programs associated with the most events.
3. Do one of the following:
   - To see a list of all events in the last 14 days, click on the graph.
   - To see a list of events associated with one of the individual event-prone programs, click the appropriate link.

   An Event Details report appears, showing a list of program event entries. By default, IAS displays entries in order of timestamp, with the most recent event appearing first.
4. Click on any underlined column heading to rearrange the table according to that heading. For example, if you want to view events according to user, click the User column heading.

## Observing programs

If you have enabled Program Observation, Integrity Advanced Server tracks the first appearance of all programs on your network on an endpoint-by-endpoint basis. Every time a program appears for the first time on an endpoint, IAS records it.

IAS lists observed programs by first observation time, showing the most recently observed program first. This gives you an up-to-date view of the programs being introduced into your network. You can search for programs by user, program, program version, publisher, and first or last observation.

When you enable Program Observation, IAS displays new programs in Program Manager at the end of each observation period. In Program Manager, you can organize these observed programs into groups to which you can then apply program rules. For general information about Program Observation, see "Observing Program Activity," on page 87. For more information about Program Manager, see "Gathering and Organizing Program Information," on page 83.

### To monitor observed programs:

1. Go to **Reports** | **Program Observation**.
2. Enter the desired filter values and click **Apply Filter**.

   The Program Observation by Endpoint report appears. You can click on any underlined column heading to sort by that column.
3. To see the Endpoint Details report for a particular endpoint, click on the desired user link. (For more information about the Endpoint Details report, see "Finding detailed information about individual endpoints," on page 182.)

# SmartSum Command-Line Switches

The SmartSum program recognizes nine command-line switches.

The following table lists the SmartSum switches and their parameters.

| Switch | Function |
|---|---|
| /o | Specifies the output file to be created. If no file name is specified, the default output file name (`scan.xml) is used`.<br>**Example 1**: `C:\appscan /o scan1.xml [files]`<br>In Example 1, the reference scan is named scan1.<br>■ The output file name is important since you will be using this file when importing it into Integrity Server as a reference source.<br>■ If you conduct multiple scans on the same machine, give each scan a unique name. |
| /x | Designates the target file names to add to the reference scan.<br>■ The leading period before a file extension is required.<br>■ A semi-colon separates the target extensions.<br>■ The target extensions are grouped by quotes.<br>■ A target directory must be specified using the /s switch.<br>■ If the `/x` switch is not used in the command statement:<br>▪ Only program files (.exe file name extension) are scanned.<br>**Example 1**: `C:\appscan /o scan2.xml /x ".exe;.dll" /s "C:\"`<br>In Example 2, the reference scan is named `scan2`, and the scan will include `.exe` and `.dll` files in the current directory only. |

| Switch | Function |
|---|---|
| /s | Designates the directory for SmartSum to inventory.<br>■ If you do not use /s to designate a target directory, the scan will be run in the current directory only.<br>■ If you use /s, the scan will be run in the target directory and its subdirectories.<br>■ The target directory must be enclosed in quotation marks.<br>**Example 3**:`C:\appscan /o scan3.xml /x ".dll" /s "c:\program files"`<br>In Example 3, the reference scan is named `scan3`. The target directory is `C:\program files` and all its subdirectories. The target extension is `.dll`.<br>**Example 4**: `C:\appscan /o scan4.xml /x ".exe;.dll" /s "c:\program files"`<br>In Example 4, the reference scan is named `scan4`. The target directory is `c:\program files`. The target extensions are `.exe` and `.dll`. |
| /e | Use the `/e` switch to inventory all executable files in the target directory or drive, regardless of extension. **Example 5**: `c:\appscan /s "C:\program files" /e`<br>In Example 5, all files are incorporated into the reference scan. |
| /a | Generates all file properties for each file inventoried.<br>**Example 6**: `c:\appscan /o scan6.xml /s "C:" /a`<br>In Example 6, the reference scan is named `scan6`. The target directory is the entire contents of c: The output file displays file properties more thoroughly than it would without the `/a` switch.<br>The `/a` switch does not affect the reference source. |
| /p | Displays progress messages. |
| /verbose | Displays progress and error messages. |
| /warnings | Displays warning messages. |
| `/?` or `/help` | Displays help for SmartSum. |

Use the following table to locate pages in the Administrator Console.

| Page Name | Location |
|---|---|
| Access Zones, Edit | Policies \| <select policy> \| Edit \| Access Zones |
| Access Zones, View | Policies \| <click policy name> \| Access Zones |
| Add Destinations to Firewall Rule | Policy Objects \| Firewall Rules \| <select rule> \| Edit \| Add |
| Add Enforcement Rules | Policies \| <select policy> \| Edit \| Enforcement Settings \| Add |
| Add Firewall Rule to Policy | Policies \| <select policy> \| Edit \| Firewall Settings \| Add |
| Add Firewall Rule to Program | Policies \| <select policy> \| Edit \| Program Rules \| <select program rule> \| Edit Settings \| Add |
| Add Locations to Zones | Policies \| <select policy> \| Edit \| Access Zones \| Add |
| Add Mailsafe Extension to Policy | Policies \| <select policy> \| Edit \| Mailsafe Rules \| Add |
| Add Program Groups | Policies \| <select policy> \| Edit \| Program Rules \| Add \| <click program group name> |
| Add Program Rules | Policies \| <select policy> \| Edit \| Program Rules \| Add |
| Add Protocols to Firewall Rule | Policy Objects \| Firewall Rules \| <select rule> \| Edit \| Add |
| Add Restriction Firewall Rules to Policy | Policies \| <select policy> \| Edit \| Enforcement Settings \| Add |
| Add Sources to Firewall Rule | Policy Objects \| Firewall Rules \| <select rule> \| Edit \| Add |
| Administrator Manager | System Configuration \| Administrators |

| Page Name | Location |
|---|---|
| Administrator, Edit | System Configuration \| Administrators \| <select administrator> \| Edit |
| Administrator, New | System Configuration \| Administrators \| New |
| Administrator, view | System Configuration \| Administrators \| <click administrator name> |
| Anti-Virus Reference Client Configuration | Client Configuration \| Reference Clients \| <select provider> \| Configure |
| Anti-Virus Reference Clients | System Configuration \| Reference Clients |
| Anti-Virus Rule, Edit | Policy Objects \| Enforcement Rules \| <select rule> \| Edit |
| Anti-Virus Rule, New | Policies \| <select policy> \| Edit \| Enforcement Settings \| Add \| New Anti-virus Rule |
| Anti-Virus Rule, New | Policy Objects \| Enforcement Rules \| New \| Antivirus Rule |
| Anti-Virus Rule, View | Policy Objects \| Enforcement Rules \| <click rule name> |
| Assign Policy | Entities \| <select catalog \| Assign Policy |
| Certificate Authority Request | System Configuration \| Certificates \| New \| CA Request |
| Certificate Authority Request, View | System Configuration \| Certificates \| <click request name> |
| Certificate Manager | System Configuration \| Certificates |
| Classic Firewall Rule Manager | Policy Objects \| Firewall Rules |
| Classic Firewall Rule, Edit | Policy Objects \| Firewall Rules \| <select rule> \| Edit |
| Classic Firewall Rule, New | Policy Objects \| Firewall Rules \| New |
| Classic Firewall Rule, View | Policy Objects \| Firewall Rules \| <click rule name> |
| Client Events Report | Old Reports \| Client Events \| Apply Filter (Available only when upgrading from a previous version of Integrity Advanced Server) |

| Page Name | Location |
|---|---|
| Client Events Report | Reports \| Client Events |
| Client Pacakage, Edit | Client Configuration \| Client Packages \| <select package> \| Edit |
| Client Package, New | Client Configuration \| Client Packages \| New |
| Client Package, View | Client Configuration \| Client Packages \| <click package name> |
| Client Packager | Client Configuration \| Client Packages |
| Client Rule, Edit | Policy Objects \| Enforcement Rules \| <select rule> \| Edit |
| Client Rule, New | Policies \| <select policy> \| Edit \| Enforcement Settings \| Add \| New Client Rule |
| Client Rule, New | Policy Objects \| Enforcement Rules \| New \| Client Rule |
| Client Rule, View | Policy Objects \| Enforcement Rules \| <click rule name> |
| Client Settings, Edit | Client Configuration \| Client Settings \| Edit |
| Client Settings, Edit | Policies \| <select policy> \| Edit \| Client Settings |
| Client Settings, View | Client Configuration \| Client Settings |
| Client Settings, View | Policies \| <click policy name> \| Client Settings |
| Client Update Report | Old Reports \| Client Update \| Apply Filter (Available only when upgrading from a previous version of Integrity Advanced Server) |
| Connectivity Report | Old Reports \| Connectivity \| Apply Filter (Available only when upgrading from a previous version of Integrity Advanced Server) |
| Connectivity Report | Reports \| Connectivity |
| Create New Policy | Policies \| New \| From Template |
| Custom Catalog Group | Entities \| <click catalog name> \| New Group |
| Custom Catalog, Edit | Entities \| <select catalog> \| Edit |
| Custom Catalog, New | Entities \| New \| Custom |

| Page Name | Location |
|---|---|
| Custom Catalog, View | Entities \| <click catalog name> |
| Customize Sandbox | Client Configuration \| Sandbox Pages |
| Endpoint Compliance History Report | Reports \| Endpoints \| Apply Filter \| <click a user name> \| Compliance State |
| Endpoint Details Report | Reports \| Endpoints \| Apply Filter \| <click user name> |
| Endpoint Report | Reports \| Endpoints |
| Enforcement Report | Old Reports \| Enforcement \| Apply Filter (Available only when upgrading from a previous version of Integrity Advanced Server) |
| Enforcement Rule Manager | Policy Objects \| Enforcement Rules |
| Enforcement Rule, Edit | Policy Objects \| Enforcement Rules \| <select rule> \| Edit |
| Enforcement Rule, New | Policies \| <select policy> \| Edit \| Enforcement Settings \| Add \| New Enforcement Rule |
| Enforcement Rule, New | Policy Objects \| Enforcement Rules \| New \| Enforcement Rule |
| Enforcement Rule, View | Policy Objects \| Enforcement Rules \| <click rule name> |
| Enforcement Settings, Edit | Policies \| <select policy> \| Edit \| Enforcement Settings |
| Enforcement Settings, View | Policies \| <click policy name> \| Enforcement Settings |
| Entity Manager, Edit | Entities |
| Entity Manager, View | Entities |
| Event Destination, Edit | System Configuration \| Event Notification \| <select destination> \| Edit |
| Event Destination, New | System Configuration \| Event Notification \| New |
| Event Details Report | Old Reports \| Client Events \| Apply Filter \| <click summary> (Available only when upgrading from a previous version of Integrity Advanced Server) |

| Page Name | Location |
|---|---|
| Event Details Report | Reports \| Client Events \| <choose a report (other than Summary or Compliance Status)> \| click Apply Filter \| <click a graph> |
| Event Manager | System Configuration \| Event Notification |
| Firewall Settings, Edit | Policies \| <select policy> \| Edit \| Firewall Settings |
| Firewall Settings, View | Policies \| <click policy name> \| Firewall Settings |
| Gateway Catalog Group | Entities \| <click catalog name> \| New Group |
| Gateway Catalog, Edit | Entities \| <select catalog> \| Edit |
| Gateway Catalog, New | Entities \| New \| Gateway |
| Gateway Catalog, View | Entities \| <click catalog name> |
| Generate Self-Signed Certificate | System Configuration \| Certificates \| New \| Self Signed |
| Import Certificate | System Configuration \| Certificates \| New \| From File |
| Import Policy | Policies \| New \| From File |
| Import Reference Source | Global Policy Settings \| Reference Sources |
| Install Certificate Authority Certificate | System Configuration \| Certificates \| New \| CA Issued Certificate |
| Integrity Monitor Report | Reports \| Integrity Monitor |
| IP Catalog Group | Entities \| <click catalog name> \| New Group |
| IP Catalog, Edit | Entities \| <select catalog> \| Edit |
| IP Catalog, New | Entities \| IP Catalog |

| Page Name | Location |
|---|---|
| IP Catalog, View | Entities \| <click catalog name> |
| LDAP Catalog, Edit | Entities \| <select catalog> \| Edit |
| LDAP Catalog, New | Entities \| New \| LDAP |
| LDAP Catalog, View | Entities \| <click catalog name> |
| Location Manager | Policy Objects \| Locations |
| Location, Edit | Policy Objects \| Locations \| <select location> \| Edit |
| Location, New | Policy Objects \| Locations \| New |
| Location, View | Policy Objects \| Locations \| <click location name> |
| Mailsafe Extension Manager | Policy Objects \| File Extensions |
| Mailsafe Extension, Edit | Policy Objects \| File Extensions \| <select extension> \| Edit |
| Mailsafe Extension, New | Policy Objects \| File Extensions \| New |
| Mailsafe Extension, View | Policy Objects \| File Extensions \| <click extension name> |
| Mailsafe, Edit | Policies \| <select policy> \| Edit \| Mailsafe Rules |
| Mailsafe, View | Policies \| <click policy name> \| Mailsafe Rules |
| Name and Notes, Edit | Policies \| <select policy> \| Edit |
| Name and Notes, View | Policies \| <click policy name> |
| NT Domain Catalog, Edit | Entities \| <select catalog> \| Edit |
| NT Domain Catalog, View | Entities \| <click catalog name> |
| NTDomain Catalog, New | Entities \| New \| NTDomain |
| Policy Manager | Policies |

| Page Name | Location |
|---|---|
| Port and Protocol Manager | Policy Objects \| Ports & Protocols |
| Program Advisor Configuration, Edit | System Configuration \| Program Advisor \| Edit |
| Program Advisor Configuration, View | System Configuration \| Program Advisor |
| Program Details | Global Policy Settings \| Programs \| <click program name> |
| Program Manager | Global Policy Settings \| Programs |
| Program Observation Report | Reports \| Program Observation |
| Program Rule Settings, Edit | Policies \| <select policy> \| Edit \| Program Rules \| <select program rule> \| Edit Settings |
| Program Rule Settings, View | Policies \| <select policy> \| Edit \| Program Rules \| <click rule name> |
| Program Rules, Edit | Policies \| <select policy> \| Edit \| Program Rules |
| Program Rules, View | Policies \| <click policy name> \| Program Rules |
| Programs Report | Old Reports \| Programs \| Apply Filter (Available only when upgrading from a previous version of Integrity Advanced Server) |
| RADIUS Catalog, Edit | Entities \| <select catalog> \| Edit |
| RADIUS Catalog, New | Entities \| New \| RADIUS |
| RADIUS Catalog, View | Entities \| <click catalog name> |
| Reference Source Manager | Global Policy Settings \| Reference Sources |
| Reference Source, Edit | Global Policy Settings \| Reference Sources \| <select reference source> \| Edit |
| Role Manager | System Configuration \| Roles |
| Role, Edit | System Configuration \| Roles \| <select role> \| Edit |
| Role, New | System Configuration \| Roles \| New |

| Page Name | Location |
|---|---|
| Role, View | System Configuration \| Roles \| <click role name> |
| Sandbox Templates | Client Configuration \| Sandbox Templates |
| Security Model | System Configuration \| Security Model |
| Self-Signed Certificate, View | System Configuration \| Certificates \| <click certificate name> |
| Server Settings, Edit | System Configuration \| Server Settings \| Edit |
| Server Settings, View | Client Configuration \| Server Settings |
| SmartDefense, Edit | Policies \| <select policy> \| Edit \| SmartDefense |
| SmartDefense, View | Policies \| <click policy name> \| SmartDefense |
| User Activity Report | Old Reports \| User Activity \| Apply Filter (Available only when upgrading from a previous version of Integrity Advanced Server) |
| User Events Report | Old Reports \| Client Events \| Apply Filter \| Users Above Average (Available only when upgrading from a previous version of Integrity Advanced Server) |
| User Name Report | Old Reports \| Enforcement \| Apply Filter \| <click user name> (Available only when upgrading from a previous version of Integrity Advanced Server) |
| Zone Rules, Edit | Policies \| <select policy> \| Edit \| Zone Rules |
| Zone Rules, View | Policies \| <click policy name> \| Zone Rules |

**act as client**
When a program initiates a connection with a remote computer.

**act as server**
When a program "listens" for connection requests from other computers.

**assign**
To create a link between a user and an enterprise policy in Assign Policy. Note that policies must be deployed before they can be assigned.

**Blocked Zone**
Access Zone containing computers and networks you do not want endpoints to connect to. Integrity client prevents any communication between endpoint computers and computers in this Zone.

**compliant**
A computer is compliant with an enforcement rule when it meets the conditions specified in the rule. Compliant computers are granted full network access.

**component**
A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

**connected enterprise policy**
A security policy defined in Policy Manager and selected by the administrator to be enforced when the endpoint is connected to the enterprise network.

**deploy**
To place an enterprise policy on the policy server, where it can be downloaded by Integrity clients.

**disconnected enterprise policy**
A security policy defined in Policy Manager and selected by the administrator to be enforced when the endpoint is disconnected from the enterprise network.

**enforcement rule**
A rule defining conditions that must be present on a protected endpoint before it is granted unrestricted network access.

**enterprise policy**
A security policy defined in Policy Manager and assigned to endpoint users.

**entity**
A child grouping within a parent, such as user catalogs or user groups.

**heartbeat**
Regular messages sent by Integrity clients to Integrity Advanced Server, containing alert counts and compliance status.

**In compliance**
A computer is in compliance with an enforcement rule when it meets the conditions specified in the rule. Compliant computers are granted full network access.

**Integrity Agent**
The Integrity client intended for use when the administrator will centrally manage security at all times. Has a limited interface and no access to personal policy settings.

**Integrity client**
The endpoint software that implements security policies assigned from Integrity Advanced Server. There are two types of Integrity client: Integrity Agent and Integrity Flex.

**Integrity Flex**
The Integrity client intended for use when the endpoint user will sometimes have control of security. Has a full user interface giving access to personal policy settings.

**Internet Zone**
Access Zone containing, by default, all computers and networks except those you have added to the Trusted Zone or Blocked Zone.

**out of compliance**
A computer is out of compliance with an enforcement rule when it does not meet the conditions specified in the rule. Computers that are out of compliance can be observed or restricted to sandbox

**permission**
The level of access an administrator is allowed for a feature protected by a privilege. For a given privilege, an administrator will have a permission of No Access, Read, or Read/Write.

**personal policy**
A security policy configured by an endpoint user in the Integrity Flex user interface.

**policy package**
A policy package consists of two enterprise policies that are packaged together, in Policy Manager. A deployed policy package centrally

manages endpoint security using different enterprise policies for when the computer is connected to or disconnected from the enterprise network.

**privilege**
The setting which controls administrator access to a feature in the Administrator Console. For a given privilege, an administrator will have a permission of No Access, Read, or Read/Write.

**reference source**
An XML file generated by the SmartSum utility, containing Smart checksums and other information about all programs found on the computer that was scanned. Reference sources are imported into Integrity Advanced Server. Once a program in a reference source is observed (using the Program Observation feature), you can apply program rules to quickly create a baseline of application control.

**referenced program**
A program found in a reference source.

**quarantine**
MailSafe quarantines incoming e-mail attachments whose filename extensions (for example, .EXE or .BAT) indicate the possibility of auto-executing code. By changing the filename extension, quarantining prevents the attachment from opening without inspection.

**role**
The collection of privileges and permissions that defines what tasks an administrator can perform in Integrity Advanced Server. An administrators role affects what screens are displayed by Integrity Advanced Server when that administrator is logged in.

**sandbox**
A secure Web server within the protected network, to which an endpoint user can be restricted when out of compliance with an enforcement rule. Sandbox pages contain information and resources the user needs to regain compliance.

**security levels**
The pre-configured High, Medium, and Low Zone rule settings that can be used to apply instant security to newly installed clients. By default, Integrity Flex, installed with High security for the Internet Zone, and Medium security for the Trusted Zone.

**SmartSum utility**
Appscan.exe, the utility that creates program reference sources by scanning for all programs on a secure or “clean” computer. Bundled with Integrity Advanced Server.

**Smart checksum**
The type of checksum that identifies programs in reference sources produced by the SmartSum utility. Smart checksum filters out

differences between operating systems that produce different MD5 checksums for the same version of the same program, thus ensuring that each program is only listed once in the Integrity Advanced Server Program Manager.

**stealth mode**
The default mode when High security is applied in Zone Rules. In stealth mode, unsolicited inbound traffic (such as port scans) receives no response, effectively rendering the protected computer invisible to intruders.

**TrueVector security engine**
The primary component of Integrity client security. It is the TrueVector engine that examines Internet traffic and enforces security rules.

**Trusted Zone**
The access zone that contains known and trusted computers and networks. Use Zone rules to apply a lower level of security to Trusted Zone traffic, in order to enable endpoints to access needed trusted resources.

**User catalog**
User catalogs are determined by the authentication system in use on the network of the protected enterprise.

**User group**
The child entity of a user catalog. A user catalog can contain any number of groups.

# Index