IBM Security

IBM Security SiteProtector System Policies and Responses Configuration Guide

Version 3.0

Note
Before using this information and the product it supports, read the information in "Notices" on page 73.

This edition applies to Version 3.0 of the IBM Security SiteProtector System and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This guide explains how to manage policies in the SiteProtector™ System using the Policy view, as well as how to manage policies at the site level for certain agents. It also explains using Central Responses to alert security managers and analysts when events occur in your site, or when SiteProtector components change status. Before you begin, you must have installed SiteProtector and any components that support agents and appliances.

Use this guide to configure and maintain policies and responses for SiteProtector and for the agents that report to SiteProtector. When you configure SiteProtector the first time, follow the process described in the *IBM Security SiteProtector System Configuration Guide*, and use this guide for the Policy Configuration stage. After you have configured your system, use this guide to maintain policies and response settings.

Intended audience

This guide is written for security managers who configure, update, and maintain policies and responses for SiteProtector. For many sites, the Security Manager is responsible only for maintaining the security of the network. For other sites, the Security Manager is also responsible for aspects of network and security administration, such as network administration and security analysis.

You must be assigned to the SiteProtector Administrator user role to perform most of the tasks in this guide.

Terminology

Terms used for security products in this document.

Term	Description
agent	The generic term for all appliances; scanners; and network, server and desktop sensors.
appliance	An inline security device on a network or gateway. Depending on the type of appliance, it can provide any combination of intrusion detection and prevention, antivirus, antispam, virtual private networking (VPN), Web filtering, and firewall functions.
scanner	An agent that scans assets for vulnerabilities and other security risks.
sensor	An agent that monitors network traffic on the network and on servers to identify and, in some cases, stop attacks.

Prerequisite and related information

Use the following documents if you have not yet installed SiteProtector and need information about SiteProtector configuration options:

Document	Contents
IBM Security SiteProtector System Installation Guide	Provides the tasks for installing SiteProtector components and optional modules. It includes information about advanced configuration tasks such as hardening third-party software security, securing database communication, and configuring failover Event Collectors.

Document	Contents
IBM Security SiteProtector System Configuration Guide	Provides the tasks for configuring the SiteProtector components after you install the SiteProtector application.
IBM Security SiteProtector System User Guide for Security Analysts	Provides background information, procedures, and recommendations for using SiteProtector to assess vulnerabilities and monitor and analyze suspicious activity on your network.
IBM Security SiteProtector System Configuring Firewalls for SiteProtector Traffic	Contains information for a Security Manager to configure firewalls so that network devices and SiteProtector System components can communicate with each other.
IBM Security SiteProtector Information Center (Help)	Contains all the procedures that you need to use SiteProtector, including advanced procedures that might not be available in a printed user document.

Locate all the SiteProtector documents as portable document format (PDF) files in the following location:

- The IBM® Security product Information Center.

Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

Before you contact IBM Support, search for an answer or a solution by using other options first:

- See the Support portfolio topic in the *Software Support Handbook* for information about the types of available support.
- Check IBM Technotes, accessible through the IBM Support Portal.

If you are unable to find an answer or a solution in the Support portfolio or in the IBM Technotes, check to be sure your company or organization has an active IBM maintenance contract, and that you are authorized to submit a problem to IBM, before you contact IBM Support.

Procedure

To contact IBM Support:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - By using IBM Support Assistant (ISA), if the Service Request tool is enabled on your product.
     - Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
   - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   - By telephone for critical, system down, or severity 1 issues. For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or is about missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a solution is delivered to you. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Part 1. Managing policies in the repository

Chapter 1. Introduction to policy management

Use the Policy view to create, edit, and deploy policies to agents or groups in SiteProtector.

When you deploy a policy to an agent, it becomes the active policy for the agent. SiteProtector components and other IBM Security agents come with default policies. You can customize these policies in SiteProtector, as well as create new policies for any of your agents.

Topics

Policy use

Use the Policy tab to create, edit, and deploy policies to agents or groups in SiteProtector.

When you deploy a policy to an agent, it becomes the active policy for the agent. SiteProtector components and other IBM Security agents come with default policies. You can customize these policies in SiteProtector, as well as create new policies for any of your agents.

There are four areas available on the left pane of the Policy tab. The table below describes the different options according to which one you select.

Table 1. Four areas of policy usage.

Node selected	Policy view
Groups and Agents	Selecting a group or agent in the left pane displays the policies currently deployed to agents in that group and allows you to configure policy inheritance for your site. The Inherited From column shows the policy hierarchy for the group or agent you select. The Deployment History pane displays information about when policies were deployed, as well as scheduled policy deployments for this group. **Tip:** Expand the **Policy Types not Deployed** list to see other available policies for the selected agent type and version that have not been deployed to this group.
Policy Repository	Selecting the Policy Repository displays all available policies for the Agent type selected. From here, you can create, edit, and deploy policies.
Shared Objects	Selecting Shared Objects displays global objects that contain resources depended on by other policies within their repository.
Locally Configured Agents	Selecting Locally Configured Agents displays a list of agents using policies deployed outside of SiteProtector. This is a temporary access point for agents whose local policies have not yet been imported into SiteProtector. You must move agents out of this area to deploy policies to them from the Policy Repository.

Policy permissions

You need permissions to create, edit, and deploy policies in the SiteProtector System.

Deploy Policy permission

Permissions to deploy policies are set at the group level. Therefore, if a user has the Deploy Policy permission for a group, he or she can deploy policies to, or remove deployments from, that group. Group permissions are hierarchical. If you grant Deploy Policy permissions to a group, that user or user group will have the same permissions in all subgroups unless you set different permissions specifically for that subgroup.

Modify policy permissions

Permissions to edit, create, and delete policies are set by agent type. They are also at the group level, but because all policies are stored in the repository, permissions must be set for the group that contains the repository they are stored in. For example, you can assign permissions to one user group to modify Security Network IPS policies, but not to modify Proventia® Desktop Endpoint Security policies in the same repository. If you use multiple repositories, you could also grant a user or user group permissions to modify a class of agent policies in one group's repository, but not in another.

Control policy permissions

The Control permission allows users or user groups to assign policy subscription groups to an agent type. They are also set for the group containing the repository they are stored in. For example, you can assign permissions to one user group to change policy subscription groups for Security Network IPS agents, but not for Proventia Desktop Endpoint Security agents.

Note: Proventia Network Enterprise Scanner has several policy types that also include a View permission. For more information, please see the Proventia Network Enterprise Scanner documentation.

Shared policy types

Some policies are shared by different agent types. A user with permissions to a shared policy type for one agent can edit that policy for all agent types.

Example: The Group Settings policy is a shared policy. If you try to access Group Setting Policy from a repository in which you have Modify permissions for at least one of the following agents, you are allowed access:

- IBM Proventia Network Multi-Function Security (MFS)
- X-Press Update Server
- IBM Security Network Intrusion Prevention System (IPS)
- Event Archiver
- IBM Security Server Protection for Linux
- IBM Security Server Protection for Windows

Note: You are not allowed access if you do not have Modify permissions for at least one of these agents.

Assigning deploy policy permissions

This topic describes how to grant Deploy Policy permissions for a user or group of users.

Procedure

1. Select a group, and then click **Object** > **Properties**.
2. Click the **Permissions** icon.
3. In the Users and/or Groups section, select the user or user group you want to assign Deploy Policy permissions.
4. For the Deploy Policy permission, click the circle in the **Control** column.
   - A black circle indicates that the user or user group can deploy policies to this group.
   - A white circle indicates that the user cannot deploy policy to this group.
5. Click the **Save** icon.

Assigning modify or control policy permissions

This topic describes how to grant users or user groups permissions to modify policies for an agent type.

Procedure

1. Select a group, and then click **Object** > **Properties**.
2. Click the **Permissions** icon.
3. In the Users and/or Groups section, select the user or user group you want to assign the permissions.
4. Expand the Agent type for which you want to grant permissions.
5. In the Policy permission section, click the circle in the **Modify** or **Control** column.
6. Click the **Save All** icon.

Chapter 2. The policy repository

Use the policy repository to create, edit, and deploy policies in SiteProtector. The repository keeps an archive of each saved version of your policies.

Topics

What is the policy repository?

The policy repository is a central archive of all the policies you create and use in your site. Each time you edit a policy, SiteProtector saves a new version in the repository. You can deploy any version of a policy to an agent or group in your site.

What you see

The top pane of the repository window displays all of the policies in your repository for the selected agent type and version. Policy types that you have not created for that agent type and version are displayed in the **Policy Types Not Created** list. You can create these policies by clicking **Create This Policy** link. The bottom pane of the repository displays the version history of the policy you select..

Each time you edit a policy, SiteProtector saves a new version in the repository. You can deploy any version of a policy to an agent or group on your Site.

You can use the default repository in SiteProtector to manage all of your policies or you can create additional repositories if you want to separate policies into different groups.

IBM Security recommended practice is to use the default repository to manage and deploy policies throughout your Site.

Note: You cannot delete a policy from the repository if you have deployed it anywhere in your Site

Working with multiple repositories

Use the default repository in SiteProtector to manage all of your policies or create additional repositories to separate different types or groups of policies.

Most Sites should need only the default repository to manage and deploy policies. Users who might want to use multiple repositories include providers of managed security services who manage Sites for multiple locations or businesses and need unique sets of policies and Shared Objects for each entity.

Creating a new repository

Create additional policy repositories to separate groups of policies and responses.

About this task

Note: You can create a new repository only in a group with no active policy deployments.

Procedure

1. Select a group for which to create the new repository, and then click **Object** > **New** > **Policy Repository.**
2. Click **Yes** on the confirmation box.
3. To copy policies from another repository, drag them from that repository's list into the new repository.

Merging policy repositories

Use the merge command to consolidate policy repositories from individual groups.

About this task

If you have created additional policy repositories in individual groups, you can merge them into the parent repository to consolidate and simplify the deployment process. Merging copies all unique policies from the merged repository into the parent repository. Policies with identical names, as well as shared objects, are merged. This means that all unique attributes of the policy or object will be added to a single policy or shared object in the parent repository. Attributes with the same name that are not identical will cause conflicts.

Important: You must resolve all conflicts for merged policies or shared objects to complete the repository merge.

Procedure

1. Select **Policy** from the Go to list.
2. Select the repository you want to merge, and then click **Action** > **Merge**.
3. Click **OK** on the confirmation window.
4. If there are conflicting attributes in your policies or shared objects:
   a. If you are merging policies with the same name that are not identical, the policy is automatically renamed by appending the name of the merged repository to the front of the policy name.
   b. If you are merging shared objects with conflicting attributes, you must delete the conflicting attributes.

      Note: Each repository can contain only one set of shared objects. If you need multiple sets of shared objects, you must use more than one repository.
5. After you have resolved all conflicts, click **OK**.

Shared objects

This topic provides information about Shared Objects.

Shared Objects are policies that contain resources depended on by other policies within their repository. A policy repository can contain only one of each type of Shared Object. However, the repository saves a new version of the object each time you make changes to it.

Note: The latest revision of a Shared Object is always effectively deployed.

Managing policies in the repository

This topic provides information about creating, editing, and deleting policies in your site.

Use the policy repository to create, edit, and delete policies in your site. You can create a new policy from a blank template or by deriving a new file using information from an existing policy in your site. You can create new versions of a policy by editing an existing policy. You cannot delete a policy from the repository if you have deployed it anywhere in your site.

Creating a new policy

You can create a new policy based on the default policy for an agent.

Procedure

1. Select the **Policy** view, and then select the Policy Repository.
2. Click **New** > **Policy**.
3. Type a **Name** for the new policy.
4. To open a blank policy template, select **Generate Empty**, and then select a **Policy Type** from the list.
5. To import a policy file, select **Import from File**, and browse to the file you want to import.
6. Click **OK**.

Deriving a new policy from an existing policy

Use the Derive New command to copy settings from an existing policy you don't want to modify into a new policy.

Procedure

1. Select the **Policy** view, and then select the **Policy Repository**.
2. Select the policy you want to copy, and then click **Action** > **Derive New**.
3. Type a name for the new policy, and then click **OK**.
4. Add or edit policy settings as needed.
5. On the **Action** menu, select **Save Policy**.
6. If you want to schedule this policy to deploy to an agent or group, select the **Deploy this New Version** check box.
7. Click **OK**.

Editing a policy

Use the Policy Repository to edit a policy. Each time you edit a policy, a new version is stored in the repository.

Procedure

1. Select the **Policy** view, and then select the **Policy Repository**.
2. Right-click the policy you want to edit, and then select **Open** from the pop-up menu.
3. Edit the policy as necessary.
4. Click **Action** > **Save**.

Results

Note: SiteProtector does not automatically deploy the updated policy. You must deploy the new version of the policy to implement your changes.

Deleting a policy

Use the Delete command to delete a policy from the repository.

Procedure

1. Select **Policy** from the **Go to** list to open the Policy view, and then select the repository.
2. Select the policy you want to delete, and then click **Edit** > **Delete**.
3. Click **Yes** on the confirmation window.

Importing or exporting a policy

You can import and export default or custom policies and responses in the policy repository.

About this task

Example: If you create a policy for an IBM Security Proventia Network IPS appliance, you can import the policy into the SiteProtectorSystem, where you can apply it to groups or other appliances. Likewise, if you create a policy for a group in SiteProtector, you can export the policy to your Security Network IPS appliance.

Procedure

1. To import a policy, perform the following steps:
   a. From the **Action** menu, select **Import**.
   b. Navigate to the policy you want to import, and then click **Import**.
2. To export a policy, perform the following steps:
   a. From the **Action** menu, select **Export**.
   b. Navigate to the location to export the file, and then click **Export**.

   Note: You can change the name of the file when you export it.

Creating a policy report

You can create a report based on the settings in the policies in your repository.

Before you begin

You must have Adobe Reader to view policy reports.

About this task

Reports are generated as Portable Document Format (PDF) files and are temporarily stored on the Application Server.

Procedure

1. Select the **Policy** view, and then select the **Policy Repository**.
2. Select a policy, and then click **Action** > **Report**. SiteProtector uses the policy name as the name of the report.
3. Optional: Type a **Description** for the report.

4. Click **OK**.

Policy deployment

This topic describes how to deploy policies from the repository to the appropriate agents or groups.

Deploying a policy to a specific agent or group overrides policy inheritance from the parent group. Removing the specific policy deployment allows the group or agent to inherit the policy from its parent group again. For more information about inheritance, see "Policy subscription groups" on page 16.

Note: For performance reasons related to the quantity of agents typically used for those agent types, you cannot deploy policies directly to certain agents. For the following agents, you must deploy policies to the group containing the agent:

- Proventia Desktop Endpoint Security
- IBM Security Server Protection for Linux
- IBM Security Server Protection for Windows

Deploying a policy from the repository

A new or edited policy will not affect agents until you deploy it to the appropriate agents or groups.

About this task

To modify policies for agents that you deployed outside of SiteProtector, you might need to import the policy into SiteProtector first.

Procedure

1. Do one of the following
   - Drag the policy icon from the repository to a group or agent in the left pane.
   - Select the policy icon in the repository, and then click **Action** > **Deploy**.

   The Deploy Policy window displays the policy you chose, and the target(s) it will be deployed to.
2. To deploy additional policies, click the **Policies** icon, and then click **Add** to select more policies.
3. Click **OK**.
4. To select a target to deploy the policy to, click the **Targets** icon, and then select the groups or agents to deploy this policy to.
5. Click the **Schedule** icon.
6. To deploy the policy immediately, select **Now**.
7. To schedule a specific date and time to deploy the policy, select **Start Time**, click the drop-down list, and then select a date and time for deployment.
8. To prompt agents to update their policy immediately upon deployment, click the Summary icon, and then select the **Force affected components/appliances to contact SiteProtector when deployment completes** check box.
9. Click **OK**.

Removing a policy deployment

Use the Remove Deployment command to remove a policy deployment from a specific agent or group.

About this task

Deploying a policy to a specific agent or group overrides the policy inheritance from the parent group. Removing the specific policy deployment allows the group or agent to inherit the policy from its parent group again.

Procedure

1. Select **Policy** from the view list.
2. Select the group or agent in the left pane, and then select the policy to remove.
3. Click **Action** > **Remove Deployment**.
4. To remove additional policy deployments, perform the following steps:
   a. Click the **Policies** icon, and then click **Add**.
   b. Select additional policies, and then click **OK**.
5. To remove the policy from multiple groups or agents, click the **Targets** icon, and then select additional groups or agents.
6. Click the **Schedule** icon.
7. To deploy the policy immediately, select **Now**.
8. To schedule a specific date and time to deploy the policy, select **Start Time**, click the drop-down list, and then select a date and time for deployment.
9. To prompt agents to update their policy immediately upon deployment, select the **Force affected components/appliances to contact SiteProtector when deployment completes** check box.
10. Click **OK**.

Recurring policy deployment

You can schedule policies to be deployed to agents or groups on your site on a recurring schedule.

If you need to change the policies that are deployed to agents or groups on your site on a regular basis, you can create a schedule to automatically deploy policies at specific times or on specific days. You can also create a schedule to remove deployments on specific days or times.

Example

You want to deploy a more restrictive firewall policy on non-business days. You can schedule the more restrictive policy to deploy weekly on Friday at 5:00 p.m. You can then schedule the less restrictive policy to deploy weekly on Monday at 8:00 a.m.

Viewing policy usages

Use the Show Usages command to identify groups and agents using a particular policy.

Procedure

1. In the policy repository, right-click a policy, and then select **Show Usages**. The Deployed tab displays the following information:

Option	Description
Target	The groups or agents this policy version is deployed to
Deployment Time	The date and time the policy was deployed to each target
Deployment By	The SiteProtector user who last deployed the policy to each target

2. Click the Scheduled tab to see deployments that are scheduled but are not yet complete:

Option	Description
Target	The groups or agents this policy is scheduled to be deployed to or removed from
Action	The scheduled action: deployment or remove deployment
Deployment Time	The time the deployment or removal is scheduled

Option	Description
Deployment By	The SiteProtector user who scheduled the action

3. Click **OK** when you are finished.

Viewing differences between policy versions

If you have multiple versions of a policy in the repository, you can select two of the versions and compare the differences between them.

About this task

You can compare the differences between any two versions of the same type of policy.

Procedure

1. Select the **Policy** view, and then select the **Policy Repository**.
2. Select a policy from the repository table or a policy version from the version history table.
3. Click **Action** > **Compare Policy**.
4. Click **Browse**, navigate to any policy of the same type, and then click **OK** t select a second version of the policy.

   Tip: You can compare any two versions of the same type of policy, including policies from other repositories.
5. Click **OK**. The Policy Comparison window lists settings that have been added, deleted, or changed from one version to the next.

   Note: Differences in table rows are displayed as additions and removals if the table data doesn't have a meaningful primary key (such as firewall rules).

Migrating agent policy versions

Use the Migrate Agent Version window to migrate older versions of Proventia appliance policies to be compatible with updated agents.

About this task

If you have upgraded some of your IBM Security appliances and you want to use the same policies you defined for your older appliances, you can migrate the older, incompatible versions of your policies to the new version. You can migrate settings only at the group level; you cannot migrate policies directly for a single appliance.

Note: If you edit policies on the older appliance after you have migrated the policies to the new appliance, you must migrate the policies again for the newer appliance to have the updated versions.

Procedure

1. Select the group that contains the upgraded appliances, and then click **Action** > **Updates** > **Migrate Agent Version**.
2. Select the **Agent Type** from the list.
3. Click the **Upgrade Details** icon, and then select the older appliance version from the **Migrate From Firmware Version** list.
4. Select the new appliance version from the **Update to Firmware Version** list.
5. If the version to which you are migrating can update itself, select the **Update Agents** check box, and then select a date and time.

6. To prompt agents to update immediately, select the **Force affected agents to heartbeat** check box.
7. Click **OK**.

Chapter 3. Working with policies at the group level

This chapter provides information about what appears in the Policy view when you select a group or agent in the left pane.

Although most policy deployment functions are done through the repository, you can still select groups and agents to see which policies are deployed there, where they are inheriting them from, and to which policy subscription groups your agents are assigned.

Note: Although some of the same policy functions are available at the group level, you should use the repository view to create and manage your policies. See "Managing policies in the repository" on page 9.

Topics

Viewing policy deployments

When you select a group or agent in the Policy view, the top pane displays details about the policies, based on the agent type and version selected, that are currently deployed to that group or agent. This includes the name and version of the policy deployed, as well as the parent group from which it is inherited.

Policies not deployed

You can expand the **Policy Types Not Deployed** list to see other available policies for the selected agent type and version that have not been deployed to this group. You can edit and deploy those policies from the repository.

Deployment history

The Deployment Jobs pane displays information about when selected policies were deployed, as well as scheduled policy deployments for this group.

Policy inheritance

Agents and assets automatically inherit policy settings from the groups above them in the hierarchy. These groups inherit policy settings from the next higher group in your site structure.

Policy inheritance is similar to Windows file permissions in that it allows you to reuse a policy without having to redefine it at each level in the tree.

Policy inheritance configures lower-level (child) agents and groups to inherit policy from parent groups. A child agent or group that inherits policy from a parent group continues to use this policy until you either specifically deploy the policy at the child agent or group level, or you move the parent or child group to a location that is outside its current hierarchy.

Overriding policy inheritance

You can override policy inheritance by applying policy to individual agents, groups, or subgroups. If you deploy a different policy to the specific subgroup or agent, that policy is no longer inherited from the parent group.

To reestablish policy inheritance, remove the deployment from the subgroup or agent. It will then automatically inherit the policy deployed to the parent group.

For more information, see "Deploying a policy from the repository" on page 11, or "Removing a policy deployment" on page 11.

Policy subscription groups

Use policy subscription groups to apply common policy settings to several agents in the same group.

Although agents can belong to more than one group in your site structure, an agent can subscribe to policies from only one group. In the policy view, an agent is displayed in its policy subscription group.

Because policies can be set at the group level, you should create at least one policy subscription group for every unique policy that you plan to deploy. You can assign any folder on a site as a policy subscription group, except the Unassigned Assets folder.

Note: Each group can have only one policy for each agent type.

When you assign an agent or group to a policy subscription group, it automatically applies any policy changes made at the group level. Policy changes are automatically sent to most agents; Desktop Endpoint Security agents receive policy updates the next time they send a heartbeat to the Agent Manager.

Assigning a policy subscription group

Use policy subscription groups to apply common policy settings to several agents in the same group.

Procedure

1. Select a group, and then select **Agent** from the view list.
2. Select the agent, and then click **Action** > **Configure Agents** > **Assign Policy Subscription Group**.
3. Select a group in the tree.

   Important: If you select **None**, the agent will be moved outside of the grouping structure and will not inherit policies from any group.
4. Click **OK**.

Chapter 4. Locally configured agents

Agents whose policies are managed locally (using Proventia Manager) are displayed in the Locally Configured Agents node. You must move agents out of this node to take advantage of the policy features available in the SiteProtector System.

Topics

The Locally Configured Agents node

The Locally Configured Agents node displays a list of agents using policies deployed outside of SiteProtector. This is a temporary access point for agents whose local policies have not yet been imported into SiteProtector.

Tip: You must move agents out of this area to take advantage of the policy features available in SiteProtector.
The Locally Configured Agents node is designed to be a temporary access point for agents whose local policies have not yet been imported into SiteProtector. You should move these policies into the policy repository to manage them in SiteProtector.

You can import the agent's policies to use in SiteProtector or move the agents and use policies from the SiteProtector repository.

What is a locally configured agent?

A locally configured agent does not inherit policy from any group. It uses policies that are located on the agent itself, and cannot take advantage of the policy management features in SiteProtector.

If the agent has a policy subscription group, the agent name is displayed in that group in the color gray, and also under the Locally Configured Agents node. After you migrate the agent into the Repository, it resides in its assigned policy subscription group.

How do my agents get there?

Agents are placed in the Locally Configured Agents node when they are added to your site, but you do not migrate their policies into SiteProtector. This often happens when you upgrade from SiteProtector Service Pack 6.x to Service Pack 7.0. You can edit the agent's policies in SiteProtector, as well as on the agent itself, but you cannot use these policies for other agents in your site.

Migrating locally configured agents into SiteProtector

You must migrate agents out of the Locally Configured Agents area to take advantage of the policy features available in SiteProtector.

Procedure

1. Select the **Policy** view, and then select **Locally Configured Agents**.
2. Select the agent, and then click **Action** > **Migrate to Repository** from the pop-up menu.

3. Select the **Import Policy** check box to import the agent's policies into the repository, and then select the policies you want to import.

   Important: If you select this option, the agent will not inherit those policies from its parent group. Any policies you do not select are deleted permanently.

   Note: Agent-specific policies are imported automatically.
4. Click **OK**. Any imported policies are stored in the Repository and can be deployed to other groups or agents in SiteProtector.

   Important: When you merge locally managed agent policies into the repository, not all policy settings will be migrated. Settings that are not list data (for example, check boxes and text fields) will automatically inherit the values set within the policy in that repository. To avoid problems, open and review the policy settings after the migration is complete.

Part 2. Configuring central responses

Chapter 5. Working with central responses

This chapter provides an overview of the Central Responses feature in SiteProtector. Central Responses provide control over responses to events and the status of components in a central location in SiteProtector.

Topics

Central responses

Use the Central Responses feature to create response rules that apply to events or component statuses that occur on your site.

If event parameters match a response rule you create, SiteProtector generates a notification in the form of an email, SNMP, or user-specified response. You can control how often this notification is generated and on what event parameters it is based.

A central response consists of a Response Rule and a Response object. The Response Rule determines when a response is initiated. The Response Object is the action taken when the rule is triggered. In addition, you can create Network Objects, which are defined segments of your network that you can reuse throughout multiple responses.

The following table describes the components of Central Responses:

Component	Description
Response Rule	Defines the criteria required to generate a response.
Response Object	Defines a particular response, such as an email to one or more individuals. You assign response objects to response rules to define the response to generate for each rule. There are five types of response objects: • Email • SNMP • Log Evidence • Quarantine • User-specified
Policy Deployment Object	Policy Deployment Objects are a special type of response that deploy pre-configured policies to groups or agents in your site when criteria for a Response Rule is met.
Network Object	Network Objects define custom network address and port lists that policies and responses can share. You can assign network objects to rules to define which assets the rule covers. **Note:** Network objects are optional. You can also define specific assets in the response rule.

Creating central responses

Use the Central Responses window to create Central Responses.

About this task

Central Responses use a rule (Response Rules) to apply responses (Response Objects or Policy Deployment Objects) to assets or agents in your site (Network Objects). However, when creating Central Responses, you might find it easier to build them in the reverse order.

Response Rules include both the Response Object (or Policy Deployment Object) that is applied by the rule and the location where the Object is applied (which can be a Network Object). Therefore, it makes sense to create any Network Objects and Response Objects you want to use before you create the Response Rule.

Procedure

1. Select **Tools** > **Central Responses** to open the Central Responses window.
2. Define any Network Objects you want to use.
3. Define the Response Object or Policy Deployment Object you want to apply.
4. Define the Response Rule to trigger the response.

Chapter 6. Defining response objects

This chapter provides information about defining Response Objects.

Topics

Response objects

When criteria for a response rule is met, SiteProtector triggers a Response Object. A response object can send an email to a responsible party, such as an incident response team or a Site Administrator, trigger an SNMP trap, log the activity, quarantine intruder activity, or run a user-specified script on the application server.

You can centralize data entry so that you need only change the response object instead of changing each instance of the data. For example, if you have set responses to email JohnS, and his email address changes, you can edit the address in the response object, rather than changing the address in every place that it appears.

Note: You can apply the response objects you create for IBM Security Network Intrusion Prevention System (IPS) in SiteProtector to local responses on the appliance.

The following table lists response objects and the agents they support:

Response Object	Security Network IPS	IBM Security Virtual Server Protection for VMware	All other Agents
Email	Yes	Yes[1]	Yes
Log Evidence	Yes	Yes	No
Quarantine	Yes	Yes	No
SNMP	Yes	Yes[1]	Yes
User-Specified	Yes	Yes[1]	Yes

[1] Supported at the SiteProtector level (through Central Responses), not at the agent level

Configuring email response objects

This topic provides information about adding, removing, and editing email Response Objects.

Description

Email Response Objects contain the information that SiteProtector sends in an email message in response to a security event. You can define the following items that are included in the email:

- Name of the email
- SMTP host
- From
- To
- Subject
- Body

Note: In the subject line and body of the email, you can include parameters, such as the following items:

- Name of the agent that detected the event
- The destination address of the security event
- The port of the security event
- The address of the agent that detected the event
- The status of the agent that detected the event
- The version of the agent that detected the event

Creating an email response object

When responses are generated on your Site, you can send an email notification to interested or responsible parties. Use email response objects to configure email addresses that you want multiple agents on your Site to share.

Procedure

1. Choose the appropriate method to create a response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **Email** tab, and then click the **Add** icon.
3. Specify the following options as needed:

Option	Description
Name	A unique name for the response object, such as `Email Response Team1`.
SMTP Host	The name of the SMTP host that will handle the email. **Tip:** The SiteProtector System supports Internationalized Domain Names (IDNs). IDNs support non-ASCII (Unicode) characters.
From	The email address from which the message will originate. **Tip:** The SiteProtector System supports Email Address Internationalization (EAI). Internationalized email addresses support non-ASCII (Unicode) characters for the domain name, which is the part of the email address that follows the @ sign. The local part of the email address that precedes the @ sign is still restricted to ASCII-only characters. An example of an internationalized email address that uses Simplified Chinese for the domain name is: mailtest@例子.测试
To	The email address where you want to send the notification. Separate multiple email addresses using semicolons. **Tip:** See the Tip above regarding Email Address Internationalization.

4. Type a subject line for the email, or select an item to include in the message in the Agent Parameters folder, and then click **Subject**.

Note: For event rules, use the Common Parameters branch. For component rules, use the Component Parameters branch.

5. Type the body of the message, or select an item to include in the message in the Agent Parameters folder, and then click Body.

   Note: If you select a parameter that does not match an event associated with a response rule, the parameter will appear in the email in the original tag format.

   Example: If you select the **<ObjectName>** parameter, and the event associated with the response in the response rule does not contain this parameter, it appears as **<ObjectName>** in the email.
6. Click **OK**.

Editing email addresses

Use the Email tab to edit an email address in the Response Objects policy.

Procedure

1. Choose the appropriate method to edit an email address for the response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **Email** tab.
3. Select the email response, and then click **Edit**.
4. Change the email address as necessary, and then click **OK**.
5. Click **Apply**.

Removing emails

Use the Email tab to remove an email from the Response Objects policy.

Procedure

1. Choose the appropriate method to remove an email address for the response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **Email** tab.
3. Select the email response, and then click **Remove**.
4. Click **Yes** in the alert window to confirm your changes.

Configuring SNMP response objects

This topic provides information about adding, removing, and editing SNMP Response Objects.

Description

An SNMP response is a response that SiteProtector sends to a SNMP manager. The response includes data from SNMP-compliant devices, called agents, about the following types of events:

- Connection events
- User-defined events
- Security events

Background

Simple Network Management Protocol (SNMP) is a set of protocols for managing networks. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return the data to SNMP management applications, such as OpenView. SNMP agents only communicate with SNMP management applications located in the same community. A community is a user-defined setting for basic authentication. The SNMP settings in the Response Objects policy define the IP address and community for the SNMP manager.

Note: The IBM Security MIB file (iss.mib) defines the format of the SNMP traps and is used by SNMP management applications to provide a translation of the numeric Object Identifiers (OIDs) in the trap messages. To display the Event Name in SNMP trap messages, import or compile iss.mib in a SNMP management application. You can download the iss.mib file from the IBM Security License Key and Download Center at https://ibmss.flexnetoperations.com/control/isdl/home.

Creating an SNMP response object

Use an SNMP Response Object to specify where to send an SNMP notification (trap). Objects you create here can be used by multiple response rules.

About this task

SNMPv3 is not available for IBM Security Virtual Server Protection for VMware agents except through Central Responses.

Procedure

1. Choose the appropriate method to create a response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **SNMP** tab, and then click the **Add** icon.
3. Specify the following options:

Option	Description
Unique Name	Specifies a meaningful name for the response. **Tip:** This name appears when you select responses for events, so give the response a name that allows users to easily identify what they are selecting.
SNMP Manager	Specifies the IPv4 or IPv6 address or the host name of the SNMP system that receives notifications.
Port Number	Specifies the port number the SNMP manager monitors for notifications (traps and informs). The default number is port 162.
SNMP Version	Specifies the SNMP version.
SNMPv1/SNMPv2c Community String	Specifies the text string password for SNMPv1 or SNMPv2c systems.
SNMPv3 Settings: User Name	Specifies the user that controls SNMPv3 notifications.

Option	Description
SNMPv3 Settings: Notification Type	Specifies the notification as a trap or an inform. • **Trap**: Specifies SNMPv3 traps for notifications. – (Optional) Enter a **Local EngineID**. This number is assigned to the local SiteProtector application that generates (sends) notifications. **Note:** This field is optional. However, the ID is needed to configure the trap receiver. If you do not create the ID using this field, you need to determine the ID that is automatically assigned by the local application. You can accomplish this by setting the Application Server logging to "DEBUG" and generating a trap. Then you can find the ID in the Application Server log file. • **Inform**: Specifies SNMPv3 informs for notifications. – (Optional) Enter a **Manager's EngineID**. This number specifies the remote engine that receives notifications and that has the authority to control the flow of information. **Note:** This field is optional. If not specified, SiteProtector attempts to contact the SNMPv3 manager engine to retrieve the ID. – Enter a **Timeout** value that specifies how long SiteProtector waits before it resends a notification due to no confirmation.
SNMPv3 Settings: Authentication	Specifies whether notifications use authentication. • **Enable Authentication**: Specifies the need for authentication. • **Password**: Specifies and confirms the password used to authenticate SNMPv3 notification messages. **Note:** This password must contain at least eight characters and is case-sensitive. • **Type**: Specifies the HMAC (hash-based message authentication code) algorithm used to authenticate SNMPv3 notification messages.
SNMPv3 Settings: Privacy	Specifies whether notifications use privacy settings. **Note:** Privacy settings cannot be enabled unless authentication is enabled. • **Enable Privacy**: Specifies whether privacy settings are enabled. • **Use Authentication Password as Privacy Password**: Allows the authentication password to be used as the privacy password. • **Password**: Specifies and confirms the password used to encrypt SNMPv3 notification messages. **Note:** This password must contain at least eight characters and is case-sensitive. • **Type**: Specifies the algorithm used to encrypt SNMPv3 notification messages.

4. Click **OK**.

Editing SNMP response

Use the SNMP tab to edit an SNMP response in the Response Objects policy.

Procedure

1. Choose the appropriate method to edit an SNMP response for the response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **SNMP** tab, and then select the SNMP response.
3. Change the setting as necessary, and then click **OK**.
4. Click **Apply**.

Removing SNMP responses

Use the SNMP tab to remove an SNMP response from the Response Objects policy.

Procedure

1. Choose the appropriate method to remove an SNMP response for the response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **SNMP** tab.
3. Select the SNMP response, and then click the **Remove** icon.
4. Click **Yes** in the alert window to confirm your changes.

Configuring user-specified response objects

This topic provides information about adding, removing, and editing user-specified Response Objects.

Important: The user-specified response must be compatible with Windows-based applications.

Description

A user-specified response is a custom response that SiteProtector generates when an event occurs. The response can include any of the following actions:

- Start an application
- Run a script
- Run other commands

Requirements

The following requirements apply to user-specified responses:

- The response must be supported on Windows-based applications.
- Scripts must be stored on the Application Server computer.
- Responses must include the complete path to the storage location on the Application Server.

Creating a user-specified response object

You can create user-specified responses to events that run a user-specified script on the application server.

Procedure

1. Choose the appropriate method to create a user-specified response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **User Specified** tab, and then click the **Add** icon.
3. Type a unique **Name** for the response object.
4. Type a **Command** to associate with the object.
5. To select a parameter, expand the Agent Parameters folder.

   Note: For event rules, use the Common Parameters branch. For component rules, use the Component Parameters branch.
6. Click **Add**.
7. Click **OK**.

Editing a user-specified response

Use the User-Specified tab to edit a user-specified response in the Response Objects policy.

Procedure

1. Choose the appropriate method to edit a user-specified response:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **User-Specified** tab.
3. Select the response, and then click **Edit**.
4. Change the response as necessary, and then click **OK**.
5. Click **Apply**.

Removing a user-specified response

Use the User-Specified tab to remove a user-specified response in the Response Objects policy.

Procedure

1. Choose the appropriate method to remove a user-specified response:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **User-Specified** tab.
3. Select the response, and then click **Remove**.
4. Click **Yes** in the alert window to confirm your changes.

Configuring log evidence response objects

This topic provides information about configuring log evidence Response Objects.

Important: These settings control the behavior of the Network IPS appliance only.

Description

Log evidence allows you to configure the appliance to log the summary of an event. The Log Evidence response creates a copy of the packet that triggers an event and also records information that identifies the packet, such as Event Name, Event Date and Time, and Event ID. Evidence logs show you what an intruder attempted to do in your network.

Creating a log evidence response object

You can create Response Objects that log events and the responses they trigger.

About this task

Note: Log evidence response objects are only supported for IBM Security Network Intrusion Prevention System (IPS) and IBM Security Virtual Server Protection for VMware.

Procedure

1. Choose the appropriate method to create a log evidence response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **Log Evidence** tab, and then click the **Add** icon.
3. Specify the following options as needed:

Option	Description
Maximum Files	Type the number of log files in the database. When the log reaches the maximum number of files, it begins again with zero (0) and overwrites over any existing information.
Maximum File Size	Type a number that indicates how large the log can get before it creates a new log file.
Log File Prefix	Type the name for the output file.
Log File Suffix	Type the file extension.

4. Click **OK**.

Creating a quarantine response object

You can create Response Objects that will block intruders when a specific series of events are triggered.

About this task

Note: Quarantine response objects are only supported for IBM Security Network Intrusion Prevention System (IPS) and IBM Security Virtual Server Protection for VMware.

SiteProtector offers three pre-defined quarantine response objects:

Object	Description
Quarantine Intruder	Fully blocks both computers involved in an attack.
Quarantine Trojan	Isolates any computer that is the victim of an attack.
Quarantine Worm	Isolates the item the worm is trying to find; for example, a SQL port.

Procedure

1. Choose the appropriate method to create a quarantine response object:
   - For IBM Security Virtual Server Protection for VMware agents only, select **Default Repository** > **Shared Objects** and then click **Response Objects**.
   - For all other agents, select **Tools** > **Central Responses**, and then click **Response Objects**.
2. Select the **Quarantine** tab, and then click the **Add** icon.
3. Type a unique **Name** for the response object.
4. Select the TCP/UDP or ICMP settings for this object.
5. Click **OK**.

Chapter 7. Defining policy deployment objects

This chapter provides information about Policy Deployment Objects, a special type of response that deploys pre-configured policies to groups or agents in your site when criteria for a Response Rule is met.

Topics

Policy deployment objects

Policy Deployment Objects are a special type of Response Object that deploy pre-configured policies to groups or agents on your site when criteria for a Response Rule is met.

You can create policy deployment objects to instruct SiteProtector to apply pre-configured policies to Intrusion Prevention System (IPS) agents when certain agent events are detected.

Example: You then create a policy deployment object to apply an IPS policy to block a specific worm. You then create a response rule that triggers your policy deployment object whenever that worm is detected. An ADS agent on your site detects worm behavior and identifies a specific worm. The policy deployment object enables an IPS policy on your IBM Security Network IPS GX-series appliance that blocks that all known IRC-managed Trojans for the suspected infected host.

Creating a policy deployment object

Use the Central Responses window to create a Policy Deployment Object.

You must complete three steps to create a Policy Deployment Object:

- Configure Deployment Object settings
- Select a policy to deploy
- Select deployment targets

Configuring deployment object settings

Use the Settings window to configure basic Policy Deployment Object settings.

Procedure

1. Select **Tools** > **Central Responses**, and then click **Policy Deployment Objects**.
2. Do one of the following:
   - Click the **Add** icon.
   - Select an existing Deployment Object, and then click the **Edit** icon.
3. On the Event Driven Deployment window, click the **Setup** icon.
4. Type a unique **Response Name**.
5. Select the **Agent Type**, **Agent Version**, and **Agent Mode** for the agent policy you want to deploy.
6. If you are using multiple repositories, select the **Repository** that contains the policy you want to deploy.

Selecting a policy to deploy

After you configure basic Policy Deployment Object settings, select the policy you want to deploy when your Response Rule criteria is met.

Procedure

1. In the Event Driven Deployment window, click the **Policies** icon.
2. Click **Add**.
3. Select the policy you want to deploy, and then click **OK**.

Selecting deployment targets

After you select the Policy you want to deploy, select the groups or agents to which you want to deploy it.

Procedure

1. On the Event Driven Deployment window, click the **Targets** icon.
2. Select the groups or agents to which you want to deploy the policy, and then click **OK**.
3. Click **OK** to exit Central Responses.

Chapter 8. Defining event rules

This chapter provides information about defining event rules, which are Response Rules based on events detected by the Event Collector.

Topics

Event rules

Event rules generate responses when specified events are detected by agents on your network.

As events occur on any agent in your site, they are matched to the rules that you have created. If an event matches a rule's criteria, the Central Responses server generates a response. You can create up to 400 rules, each containing up to 50 events.

Example: You can add an event to a rule that includes all HTTP events with a high priority. When an HTTP event with a high priority occurs, SiteProtector will generate a response.

The following are examples of event rules:

- When Event_Name occurs on IP address 127.0.0.1 and targets IP address 192.0.2.0 one time in 60 seconds, SiteProtector must send an email to the site administrator that includes detailed information about the event.
- When any event occurs on any IP address within the range of 192.0.2.0-192.0.2.24 range, SiteProtector must respond with a user-specified response.
- When Event_Name occurs on port 339 on any IP address within the range of 192.0.2.0-192.0.2.24, SiteProtector must generate an SNMP response.

Adding event rules

This topic explains how to manually add an event rule and run the Add Response Rules Wizard to automatically add an event rule.

Required information

When you manually add an event rule, you must define the following information:

- the event, including event name, status, and priority
  See "Defining event filters in event rules" on page 35.
- the source IP address(es) and port(s) associated with the event
  See "Defining source addresses and source ports in event rules" on page 36.
- the destination IP address(es) and port(s) associated with the event
  See "Defining destination addresses and destination ports for event rules" on page 37.
- the response SiteProtector generates when an event matches the criteria specified in the event rule
  See "Defining responses in event rules" on page 38.
- custom, user-defined parameters for the event rule
  See "Defining advanced filters for event rules" on page 38.

Manually adding event rules

Use Event Rules tab to manually add an event rule.

Procedure

1. Click **Tools** > **Central Responses**, and then click Response Rules.
2. Select the **Event Rules** tab, and then click **Add**. The Add Event Rules window appears.
3. Select the **Enabled** check box.
4. Define the following fields:

Field	Description
Name	Provide a name of up to 50 characters in length for the event rule.
Comment	Provide a description for the event rule.
Rule Threshold	Select this option if you want to define how often the criteria in the event rule must be met before SiteProtector generates the response. **Example:** Send a response if the rule is triggered one time in 60 seconds.

5. Complete the following tasks as necessary:

Task	Reference
Define event details on the **Event** tab.	See "Defining event filters in event rules" on page 35.
Define source addresses and ports on the **Source** tab.	See "Defining source addresses and source ports in event rules" on page 36.
Define destination addresses and ports on the **Destination** tab.	See "Defining destination addresses and destination ports for event rules" on page 37.
Define the responses SiteProtector generates when an event matches the criteria specified in the event rule on the **Responses** tab	See "Defining responses in event rules" on page 38.
Define custom, user-defined parameters on the **Advanced Filters** tab.	See "Defining advanced filters for event rules" on page 38.

Automatically adding event rules

Use the Add New Response Rule Wizard to add an event rule automatically.

Procedure

1. In the left pane, select the Site Group.

   Note: Make sure you have **Show Subgroups** enabled to view all events in the site.
2. In the **View** list, select **Analysis**.
3. In the **Analysis View** list, select **Event Analysis - Details**.

   Tip: Perform this procedure on the Event Analysis - Details view. If you perform this procedure on other Analysis views, then the Wizard cannot automatically populate all required fields in the event rule.
4. Select up to 50 events on which to base the response rule.
5. Right-click the selected event(s), and then select **New Response Rule** from the pop-up menu. The Add New Response Rule Wizard begins.
6. Type a **Name** for the response rule, and then click **Next**.

   Note: To edit the information, select the rule, and then click **Edit**.
   The Event Rules tab appears with information about the event.
7. Click **OK**.

Defining event filters in event rules

This topic describes how to specify event filters in event rules.

As events occur on any sensor or appliance in your site, they are matched to the rules that you have created. When an event matches a rule's criteria, SiteProtector determines if all the other parameters also match. If all parameters match the rule, SiteProtector generates a response.

Note: You can associate up to 50 events with each response rule.

Example

You can add an event to a rule that includes all HTTP events with a high priority. When an HTTP event with a high priority occurs, SiteProtector will generate a response.

Specifying event filters

Specify the event filters that will trigger the response.

About this task

Procedure

1. On the Events tab, click the **Add** icon.
2. Select the **Enabled** check box.
3. Specify the following event information

Option	Description
Event	The event name that will match the rule (wildcards allowed).
Priority	The priority an event must have to match the rule (high, medium, low).
Status	The status of the event to match the rule.

Defining source addresses and source ports in event rules

This topic explains how to define source addresses and source ports in event rules.

Purpose

The purpose of this procedure is to associate events with source addresses and ports. The event source address and port must match the information you specify in this procedure before SiteProtector generates a response.

About back door response events

If you use back door response events to set up a rule, and you specify source and destination IP addresses, the source and destination IP addresses will be reversed on the Sensor Analysis tab:

- The source IP address is displayed in the destination IP address column (or as the victim).
- The destination IP address is displayed in the source IP address column (or as the attacker).

Specifying source IP addresses and ports

When you specify a rule's event source, you are associating events with specific source IP addresses or ports. The Central Responses server only generates a response if the event source matches an IP address and port you specified.

Procedure

1. In the **Add Event Rules** window, select the **Source** tab.
2. To include events from all IP addresses, select **Any**. Otherwise, select **Use Specific Source Address**, and then select a **Mode** from the list:

Option	Description
From	Includes events only from the IP addresses you specify
Not From	Excludes events from the IP addresses you specify

3. In the **Specific Sources** section, select one of the following options:

Option	Description
IP Address List	Applies the rule to specific IP addresses
Network Address/#Network Bits (CIDR)	Applies the rule to a block of IP addresses. **Value:** The entry after the slash is the prefix length and is a number from 1 to 32. Example: 127.0.0.1/24
IP Address Range	Applies the rule to IP addresses within a specified range. **Important:** Do not use 0.0.0.0-255.255.255.255 as the site range. If you use this as the site range, random IP addresses are added to your ungrouped assets folder, such as IP addresses from Web sites.
Address List Entry	Applies the rule to a Network Object Address Name selected from the list.

4. In the Source Port section, select one of the following options:

Option	Description
Any	Includes all ports in your site
Single Port	Includes a single port in your site
Port Range	Includes a specified range of ports **Value:** 0 to 65535.
Port List Entry	Includes a Network Object Port Name.

Defining destination addresses and destination ports for event rules

This topic explains how to define destination addresses and destination ports in event rules.

Purpose

The purpose of this procedure is to associate events with destination addresses and ports. The event destination address and port must match the information you specify in this procedure before SiteProtector generates a response.

About back door response events

If you use back door response events to set up a rule, and you specify source and destination IP addresses, the source and destination IP addresses will be reversed on the Sensor Analysis tab:

- The source IP address is displayed in the destination IP address column (or as the victim).
- The destination IP address is displayed in the source IP address column (or as the attacker).

Specifying destination IP addresses and ports

When you specify a rule's event destination, you are associating events with specific destination IP addresses or ports. The Central Responses server only generates a response if the event destination matches an IP address and port you specified.

Procedure

1. From the **Add Event Rules** window, select the **Destination** tab.
2. In the Destination Address section, select one of the following options:

Option	Description
Any	Applies the rule to events from all IP addresses.
IP Address List	Applies the rule to specific IP addresses
Network Address/#Network Bits (CIDR)	Applies the rule to a block of IP addresses. **Value:** The entry after the slash is the prefix length and is a number from 1 to 32. Example: 127.0.0.1/24
IP Address Range	Applies the rule to IP addresses within a specified range. **Important:** Do not use 0.0.0.0-255.255.255.255 as the site range. If you use this as the site range, random IP addresses are added to your ungrouped assets folder, such as IP addresses from Web sites.
Address List Entry	Applies the rule to a Network Object Address Name selected from the list.

3. In the Destination Port section, select one of the following options:

Option	Description
Any	Includes all ports in your site
Single Port	Includes a single port in your site
Port Range	Includes a specified range of ports **Value:** 0 to 65535.
Port List Entry	Includes a Network Object Port Name.

Defining responses in event rules

This topic explains how to select a response in event rules.

When an event occurs that matches a response rule, SiteProtector can send an email to a responsible party, such as an incident response team or a site administrator, it can generate an SNMP response, or it can run a user-specified script on the application server.

Note: The Response Frequency threshold is determined using the local time on your application server. If the local time on the application server is reset for any reason, response frequency might be met, and additional responses can be generated.

Specifying responses

Use this tab to select which responses are triggered when an event meets the rule criteria.

Procedure

1. Select the **Responses** tab.
2. To set a frequency for the event, type or select the appropriate values for Send at most [n] responses within [n] [time period].

   Note: If you do not specify a response frequency, then SiteProtector sends a notification every time the rule is matched. The Response Frequency threshold is determined using the local time of your Application Server. If the local time at the Application Server is reset for any reason, response frequency may be met and additional responses may be generated.
3. In the Responses section, select the responses under each tab to be generated when the rule is matched.

   Note: You create the email, SNMP, and user-specified responses that are displayed in response objects on the Responses tab. If you do not see the email or SNMP information you want to associate with this rule in the list, click **Manage Responses** to add it to the list.

Defining advanced filters for event rules

This topic explains how to add advanced filters to an event rule.

Definition

An *advanced filter* is made up of attribute-value pairs (AVPs) used to define information about the event. Some AVPs are created for you automatically when you create the event rule. For example, when you create an event rule and specify 127.0.0.1 as the source IP address, an AVP is created for you automatically with the following attribute-value pair:

- the attribute (parameter) is SourceAddress
- the value is 127.0.0.1

You can add other AVPs for the event rule as necessary. For example, you can manually add AVPs for user name or sensor name.

Note: Some event details are displayed in the Analysis tab. This allows you to see the parameters/values that are available to you. After you create a rule using the Wizard, the values are automatically populated.

Guidelines

When creating AVPs, use the following guidelines:

- Attributes (parameters) should be unique.
- Wildcard characters are not allowed.
- Do not use any of the following because these attributes can be defined in the Events, Source, and Destination tabs:
  - AlertName
  - SourceAddress
  - SourcePort
  - DestinationAddress
  - DestinationPort

Adding advanced filters

You can use attribute-value pairs (AVP) to create custom parameters that determine when an event should generate a response.

About this task

Assigning inappropriate settings to advanced filter pairs can have significant negative effects on SiteProtector's behavior.

Example

You can look for specific items, such as user names or sensor names associated with an event. As you create your response rule, you are defining some attribute-value pairs automatically. For example, when you specify a source IP address such as 127.0.0.1, you are actually creating the attribute-value pair with the parameter SourceAddress and the value 127.0.0.1.

Procedure

1. Select the **Advanced Filters** tab, and then click the **Add** icon.
2. In the **Add/Edit window** select the **Enabled** check box to enable the attribute-value pair immediately.
3. Do one of the following
   - For event rules, type a **Parameter**
   - For component rules, select **ComponentName**, **ComponentVersion**, or **ComponentHostName**.
4. Type the Value to associate with the parameter; for example, "BobW," and then click **OK**.

   Note: If the parameters and values in the event do not exactly match those specified, the server will not generate a response.
   - Parameter and Value names cannot have spaces.
   - The parameter field should be unique.
   - The following parameters are not allowed because they can be configured in the Events tab, Source tab, and Destination tab: AlertName, SourceAddress, SourcePort, DestinationAddress, and DestinationPort.
   - Wildcard characters are not allowed.

Working with event rules

This topic explains how to perform the following tasks in the Response Rules policy:

- Enable and disable event rules
- Edit event rules
- Remove event rules
- Ordering event rules

Rule order

SiteProtector implements event rules in the order you specify. The event rule's location in the list determines the order in which it is implemented. When you create new event rule, the rule is automatically positioned in the event rule list as follows:

- If you select an event rule before you create the new response rule, the new event rule is placed above the rule you selected.
- If no rule is selected at the time you create the event rule, the new event rule is placed in the last position in the list.
- If you use the Rule Wizard to create the event rule, the new event rule is placed at the first position in the rule list.

Enabling and disabling event rules

Use the Event Rules tab to enable and disable an event rules in the Response Rules policy.

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select the **Enabled** check box to enable the event rule, or clear the check box to disable the rule.
4. Click **OK**.

Editing event rules

Use the Event Rules tab to edit a response rules in the Response Rules policy.

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select the rule you want to edit, and click the **Edit** icon
4. Edit the rule as necessary.
5. Click **OK**.

Removing event rules

Use the Event Rules tab to remove an event rule in the Response Rules policy.

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select the rule you want to edit, and click the **Delete** icon.

Ordering event rules

Use the Event Rules tab to change the order of response rules.

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select a rule in the list, and then click the **Move Up** or **Move Down** options on the toolbar to change the order of the rule in the list.
4. Click **Apply**.

Customizing the event rules tab

Use the Event Rules tab to customize how rules are displayed on this tab to help you find important information when you need it.

Adding or removing columns

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab, and then click **Select Columns**.
3. Select the check box beside the column you want to add or remove from the view.
4. Click **OK**, and then click **OK** on the Central Responses window.

Sorting information in a column

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Click the column header for the column you want to sort. The information is sorted alphabetically or numerically within the column.
4. Click **OK**.

Grouping rules by column

Procedure

1. Click **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab, and then click **Group By**.
3. In the **All Columns** list, select the column you want to use to group information.
4. Click **Add**.

   Tip: You can also right-click any column heading, and then click **Group by** on the pop-up menu to group rules by column.

   Each column you add to the list is nested under the previous column. To change how columns are nested, you must remove them from the list, and then add them back to the list in the order you want.
   The column name appears in the Group by These Columns list.
5. Click **OK**.

Chapter 9. Defining component rules

This chapter provides information about defining component rules, which are Response Rules based on status changes in SiteProtector components and agents.

Topics

Component rules

Use the Component Rules tab to define the criteria to generate responses based on the status of a SiteProtector component.

As the status of a component changes, the status is compared to the component rules that you have created. If the component status matches a rule's criteria, the Central Responses server generates a response.

You can create up to 100 component rules.

Creating component rules

This topic describes how to create rules that generate responses when components report a change in status.

When you create component rules, as the status or state of a component changes, it is matched to the component rules that you have created. If a status on a component matches a rule's criteria, then SiteProtector determines if all the other parameters match as well. If all parameters match the rule, SiteProtector generates a response.

Task overview

The following table describes the tasks required to create a component rule:

Task	Description
1	Set up rule details such as name.
2	Specify filters for the rule.
3	Specify the component address for the rule.
4	Specify the response for the rule.
5	Specify advanced filters for the rule.

Specifying component rule general settings

Use the general settings to enable the component rule and describe the rule.

Procedure

1. Select **Tools** > **Central Responses**, and then click **Response Rules**.
2. Select the **Component Rules** tab, and then click the **Add** icon.

3. Specify the following options as needed:

Option	Description
Enabled	Enables the rule **Note:** You must enable the rule to edit it.
Order	Read-only field **Note:** If you select a rule before you click Add, SiteProtector adds the new rule above the selected rule. Otherwise, it adds the rule to the end of the list.
Name	A unique name for this rule. **Format:** Maximum 50 characters
Comment	Any important information about this rule. **Format:** Maximum 255 characters

Specifying component filters

Use this tab to specify what component statuses will generate a response.

About this task

You can specify filters to generate a response when the status of any SiteProtector component changes. Because the site database can reach capacity quickly in enterprise environments, there is a specific filter to generate a response when SiteProtector purges the database or when the database size exceeds the thresholds that you specify.

Procedure

1. In the Add Component Rules window, select the **Filter** tab.
2. To create a database status notification, select **Database Status Notification** from the drop-down list, and then select one or both of the following check boxes to generate the notification:
   - Enable Size Threshold Exceeded Notification
   - Enable Purge Notification
3. To create a status notification for another component, select **Component Status Notification** from the drop-down list, and then select the check boxes for the component types on which the status must occur to trigger the rule.

Specifying component addresses

Use this tab to associate filters with specific component IP addresses. The Central Responses server only generates a response if the component IP address matches an IP address you specified.

Procedure

1. In the Add Component Rules window, select the **Component Address** tab.
2. Specify the following information as needed:

Option	Description
Any	Applies the rule to any component IP address.
Single IP Address	Applies the rule to a single specified component IP address.
IP Address List	Applies the rule to a specific component IP addresses in the list.
Network Address/#Network Bits (CIDR)	Applies the rule to a block of IP addresses. **Value:** The entry after the slash is the prefix length and is a number from 1 to 32. Example: 127.0.0.1/24

Option	Description
IP Address Range	Applies the rule to IP addresses within a specified range. **Important:** Do not use 0.0.0.0-255.255.255.255 as the site range. If you use this as the site range, random IP addresses are added to your ungrouped assets folder, such as IP addresses from Web sites.
Address List Entry	Applies the rule to a Network Object Address Name selected from the list.

Specifying responses

Use this tab to select which responses are generated when a component's status meets the rule criteria.

Procedure

1. Select the **Responses** tab.
2. To set a frequency for the event, type or select the appropriate values for Send at most [n] responses within [n] [time period].

   Note: If you do not specify a response frequency, then SiteProtector sends a notification every time the rule is matched. The Response Frequency threshold is determined using the local time of your Application Server. If the local time at the Application Server is reset for any reason, response frequency may be met and additional responses may be generated.
3. In the Responses section, select the responses under each tab to be generated when the rule is matched.

   Note: You create the email, SNMP, and user-specified responses that are displayed in response objects on the Responses tab. If you do not see the email or SNMP information you want to associate with this rule in the list, click **Manage Responses** to add it to the list.

Adding advanced filters

You can use attribute-value pairs (AVPs) to create custom parameters that determine when an event should generate a response.

About this task

Assigning inappropriate settings to advanced filter pairs can have significant negative effects on SiteProtector's behavior.

Example

You can look for specific items, such as user names or sensor names associated with an event. As you create your response rule, you are defining some attribute-value pairs automatically. For example, when you specify a source IP address such as 127.0.0.1, you are actually creating the attribute-value pair with the parameter SourceAddress and the value 127.0.0.1.

Procedure

1. Select the **Advanced Filters** tab, and then click the **Add** icon.
2. In the **Add/Edit window** select the **Enabled** check box to enable the attribute-value pair immediately.
3. Do one of the following
   - For event rules, type a **Parameter**
   - For component rules, select **ComponentName**, **ComponentVersion**, or **ComponentHostName**.
4. Type the Value to associate with the parameter; for example, "BobW," and then click **OK**.

Note: If the parameters and values in the event do not exactly match those specified, the server will not generate a response.

- Parameter and Value names cannot have spaces.
- The parameter field should be unique.
- The following parameters are not allowed because they can be configured in the Events tab, Source tab, and Destination tab: AlertName, SourceAddress, SourcePort, DestinationAddress, and DestinationPort.
- Wildcard characters are not allowed.

Chapter 10. Defining network objects

This chapter provides information about defining Network Objects. You should define Network Objects before you configure policies for agents that you want to use them.

Topics

What are network objects?

Network Objects store frequently used IP addresses, ports, and other information in a single, reusable object. Network Objects provide a central location for managing this information.

If a Network Object is used by three agents, then you only need to update the information once, and the information will be updated for all three agents simultaneously.

Note: Network Objects appear in the Shared Objects node of the Policy repository. Central Responses can only use Network Objects that are stored in the default repository. For more information about Shared Objects, see "Shared objects" on page 8.

Information in network objects

Network Objects can include the following information:

- Address names
- Address groups (for IBM Proventia Network MFS responses only)
- Port names
- Port groups (for IBM Proventia Network MFS responses only)
- Dynamic address list (for IBM Proventia Network MFS responses only)

Advantages

Network Objects provide the following advantages:

- They capture a complex set of frequently used information, such as IP addresses, in a single, reusable object. The policy can be used at any time during policy and response configuration.
- They eliminate the need to re-enter large amounts of information each time you create a security policy and response.

- They provide an efficient method for updating information, such as IP addresses and ports, used in policies and responses. You change the information once, and the changes are reflected anywhere the Network Object is used.

Simple and complex objects

Network Objects can be simple or complex depending on your requirements. The most simple object contains a single IP address or port. For example, if you often use the IP address 127.0.0.1, then you can define the object to include the single IP address 127.0.0.1. More complex network objects contain a combination of information, such as a range of IP addresses and a range of ports. For example, you create a Network Object called *Boston Web Servers* that includes all of the following information:

- IP address range of 192.0.2.0 - 192.0.2.24
- Port range of 100 - 300

Task overview

The following table describes the tasks for defining a Network Objects policy:

Task	Description
1	Define address names in the policy. See "Defining address names in network objects."
2	Define address groups in the policy. See "Defining address groups in network objects" on page 49.
3	Define ports in the policy. See "Defining port names in network objects" on page 50.
4	Define port groups in the policy. See "Defining port groups in network objects" on page 51.
5	Define dynamic address names in the policy. See "Defining dynamic address names in network objects" on page 52.

Defining address names in network objects

This topic provides information about configuring address names in Network Objects.

When you edit or remove an address name and the address name is associated with response rule, you clear the association between the address name and the response rule. To restore the association, you must perform one of the following steps:

- Manually associate the response rule with the edited address name
- Create a new association between the response rule and another address name

Configuring address names

Use the Address Names tab to configure address names.

About this task

An address name is an object that includes one or all of the following items:

- Any IP address
- A single IP address

- A single IP address range
- A single IP address and CIDR mask
- A single address list

Note: An address list can contain more than one IP address range.

Important: If you edit or remove an address group from the list, any associations with this object are removed. To restore those associations, you must manually associate those response rules with a new Address Name.

Procedure

1. Select the Address Names tab.
2. Perform one of the following steps:
   - Click **Add**.
   - Select an existing address name, and then click **Edit**.
3. Type a descriptive **Name**.

   Important: You must type the name without spaces.
4. Type a description for this address name in the **Comment** box.
5. Complete one of the following tasks:

To add...	Then select...
Any IP address	**Any**.
One IP address	**Single IP Address**, and then type the IP Address in the form *x.x.x.x*.
An IP address range	**Address Range**, and then type the first and last IP address in the range in the IP Address Range fields.
An IP address on a subnet	**Network Address/#NetworkBits (CIDR)**, and then type the IP address and mask. The mask is the network identifier, and is a number from 1 to 32. **Example:** `128.8.27.18 / 16`
An address list	**IP Address List**, and then select an entry from the Address Range list. **Tip:** You can also add an address range by clicking **Add**.

6. Click **OK**.

Defining address groups in network objects

This topic provides information about configuring address groups in Network Objects.

Description

An *address group* represents the following information:

- A single address name network object
- Multiple address name network objects
- Other address groups

Note: The IBM Proventia Network Multi-Function Security (MFS) is the only agent that uses address groups.

Configuring address groups

Use the Address Groups tab to configure address groups. An address group includes one or more address names or groups.

About this task

If you edit or remove an address group from the list, any associations with this object are removed. To restore those associations, you must manually associate those response rules with a new Address Group.

Procedure

1. Select the Address Groups tab, and then perform one of the following steps:
   - Click **Add**.
   - Select an existing address group, and then click **Edit**.
2. Type a descriptive **Name** for the group.

   Important: You must type the name without spaces.
3. Type a description of the group in the **Comment** field.
4. In the Addresses area, click **Add**.
5. Do one of the following tasks:
   - Select **Address Name**, and then select a name from the list.

     Tip: Click **Address Names** to create a new address name and add it to the list.
   - Select **Dynamic Address Name**, and then select a name from the list.

     Tip: Click **Dynamic Address Names** to create a new Dynamic Address Name and add it to the list.
   - Select **Address Group**, and then select one from the Group list.
6. Click **OK**.
7. When you have finished adding addresses to the group, click **OK**.

Defining port names in network objects

This topic provides information about configuring port names in Network Objects.

Description

The following agents use port names in Network Objects:

- Event Archiver
- Central Responses
- IBM Proventia Network MFS responses

Configuring port names

Use the Port Names tab to configure port names.

About this task

A port name is a network object that includes a single port, or one or more port ranges.

Important: In the policy editor, use the Network Objects Port Names tab to configure port names. If you edit or remove a port name that is associated with policies or responses, those associations are removed. To restore those associations, you must manually associate those network objects with a new port name.

Procedure

1. Select the **Port Names** tab.
2. Perform one of the following steps:
   - Click **Add**.

- Select an existing port name, and then click **Edit**.

3. Type a descriptive **Name** for the port name.
4. Type a description for the list in the **Comment** box.
5. From the **Protocol** list, select one of the following options:

Option	Description
TCP	Transmission Control Protocol (TCP) applies to connections between two hosts that exchange streams of data.
UDP	User Datagram Protocol. Used for UNIX traceroute commands. UDP allows direct sending and receiving of datagrams over a connectionless IP network.

6. In the Port area, complete one of the following steps:
   - Select **Single Port**, and then type a port value in the **Single Port** box.
   - Select **Port Range**, and then select a port range from the **Range** list.

   Tip: You can add a Port Range by clicking **Add** in the Port Range area.
7. Click **OK**.

Defining port groups in network objects

This topic provides information about configuring port groups in Network Objects. The IBM Proventia Network Multi-Function Security (MFS) is the only agent that uses port groups in Network Objects.

When you edit or remove a port group and the port group is associated with a response rule, you clear the association between the address name and the response rule. To restore the association, you must perform one of the following steps:

- Manually associate the response rule with the edited address name
- Create a new association between the response rule and another address name

Configuring port groups

Use the Port Groups tab to configure port groups.

About this task

A port group is network object that includes one or more port names or port groups.

Important: If you edit or remove a port group that is associated with responses or policies, those associations are removed. To restore those associations, you must manually associate those network objects with a new port group.

Procedure

1. Select the Port Groups tab, and then perform one of the following steps:
   - Click **Add**.
   - Select a Port Group, and then click **Edit**.
2. Type a descriptive **Name** for the group.
3. Type a description of the list in the **Comment** box.
4. In the Ports area, click **Add**.
5. Complete one of the following steps:
   - Select **Port Name**, and then select an entry from the Port list.
   - Click **Port Names** to create or select a new port name.

- Select **Port Group**, and then select an entry from the group list.

6. Click **OK** to close the Add Ports window.
7. Click **OK** to close the Add Port Groups window.

Defining dynamic address names in network objects

This topic provides information about configuring dynamic address names in Network Objects.

Description: dynamic address name

A *dynamic address name* represents multiple dynamic address lists from different Proventia Network Multi-Function Security (MFS) appliances. Before the dynamic address name can represent the multiple lists, you must associate the dynamic address name with the different dynamic address lists. You perform this task with the IBM Proventia Network MFS interface, not in SiteProtector.

Description: dynamic address list

A *dynamic address list* represents addresses specific to IBM Proventia Network MFS. The IBM Proventia Network MFS-specific addresses are associated with a dynamic address name. A dynamic address list appears only when you access the policy editor with the Proventia Manager.

Default dynamic address names

The following table describes the default dynamic address names included in the Network Objects policy:

Name	Description
CORP	The CORP dynamic address name automatically stores the IP address and subnet mask for the IBM Proventia Network MFS internal interface. When you upgrade the IBM Proventia Network MFS firmware, the upgrade process migrates this information to the new system. For new IBM Proventia Network MFS, you must enter this information during the appliance setup process.
DMZ	The DMZ dynamic address name does not automatically store any information about the IBM Proventia Network MFS. When you upgrade the IBM Proventia Network MFS firmware, the upgrade process automatically migrates this information to the new system. For new IBM Proventia Network MFS appliances, you must enter this information during the appliance setup process.

Tasks overview

The following table describes the tasks for creating a single dynamic address name that represents multiple dynamic address lists:

Task	Description
1	Add a dynamic address name.
2	Add a dynamic address list that includes the IP addresses for each IBM Proventia Network MFS appliance.
3	For each IBM Proventia Network MFS appliance, associate the IP address for the appliance with the dynamic address list.

Configuring dynamic address names

Use the dynamic address names network object to specify one name to associate with multiple unique dynamic address lists from appliances in your site.

About this task

You associate dynamic address names with dynamic address lists at the appliance level.

Important: If you edit or remove a Dynamic Address Name associated with response rules, those associations are removed. To restore those associations, you must manually associate those response rules with a new Dynamic Address Name.

Procedure

1. Select the Dynamic Address Names tab.
2. Perform one of the following steps:
   - Click **Add**.
   - Select an existing dynamic address name, and then click **Edit**.
3. Type a descriptive **Name**.

   Important: You must type the name without spaces.
4. Type a unique description in the **Comment** box.
5. Click **OK**.

Importing and exporting network objects

If you use multiple policy repositories, you can export Network Objects from one repository and import them into another.

Procedure

1. Open a Policy tab, and then expand the repository from which you want to export the Network Object.
2. Expand **Shared Objects** > **Network Objects**.
3. Right-click the Network Objects policy, and then select **Export** from the list.
4. Type a **Name** for the object.
5. Navigate to the location where you want to save the object, and then click **Save**.
6. Expand the repository where you want to import the Network Object, and then expand **Shared Objects** > **Network Objects**
7. Right-click the Network Objects policy, and then select **Import** from the list.
8. Navigate to the saved object, and then click **Open**.

Part 3. Configuring site-level policies and responses

Chapter 11. Configuring site-level policies

Some agents use non-hierarchical policies that you can manage at the site level.

These agents include:
- IBM Internet Scanner
- IBM RealSecure Server Sensor
- SecurityFusion™ Module

Topics

What are policies?

This topic explains policies.

Policies control the following agent behaviors:
- the type and volume of security events that an agent detects
- the priority of security events that the agent detects
- the agent's response to security events

Methods for applying policies

The following table describes the methods for applying policies to Server Sensors and IBM Security Network IPS G-series appliances:

Method	Description
Apply the policy to an individual agent	You apply the policy directly to the individual agent. See "Applying policy files to agents" on page 59.
Apply the policy to a group	You apply the policy to the group that contains the agent. SiteProtector applies the policy to all agents contained in the group. **Note:** The Site Group, also called the top level group in the site, is considered a group. You can apply policies to agents at the Site Group. See "Applying policies to groups" on page 60.

Method	Description
Apply the policy to a policy subscription group	You apply the policy to a group that is assigned to an agent to serve as the agent's policy subscription group. The agent gets its policy from the policy subscription group. See "Applying policies with policy subscription groups" on page 61.

How policies are applied to different agents

The following table describes how policies are applied to different agents:

Table 2.

Agent	Description
IBM RealSecure Server Sensor	You can apply policies to these agents as follows: • Apply the policy directly to the individual agent. See "Applying policy files to agents" on page 59. • Apply the policy to a group of agents. See "Applying policies to groups" on page 60. • Apply the policy with a policy subscription group.
IBM Security Network IPS	
Proventia Desktop Endpoint Security agent	Desktop Protection agents subscribe to another group for their policies. This feature is called a *policy subscription group*. See "Applying policies with policy subscription groups" on page 61.
IBM Internet Scanner	You apply policies to the IBM Internet Scanner jobs each time you run the scan. You do not apply policies directly to the IBM Internet Scanner or to a group of scanners.

Site-level policy editor

For the following agents, you create and manage custom policies with the site-level policy editor:

- IBM RealSecure Server Sensor 7.0
- IBM Security Network IPS

Note: The site-level policy editor allows you to edit policies individually. You cannot, however, edit *multiple* policies using the site-level policy editor.

Accessing the site-level policy editor

You can access the site-level policy editor at the Site Node level or at the individual agent level in the Console.

To access the site-level policy editor:

- Select the Site Node, and then click **Action** > **Manage Policy**.

  Note: The Site Node appears as either of the following in the left pane:
  - localhost
  - IP address of the Application Server

Using the site-level policy editor

The following table lists where you can find help for topics such as customizing, printing, and applying policies with the site-level policy editor:

Product	Help for Policy Editor
IBM Internet Scanner	Network Internet Scanner Policy Editor Help
IBM Security Network IPS	Response, Policy, and Event Collector Help
Proventia Desktop Endpoint Security	Proventia Desktop Policy Editor Help
SecurityFusion Module 2.1	SecurityFusion Module Policy Editor Help
IBM RealSecure Server Sensor 7.0	Response, Policy, and Event Collector Help

Configuring custom policies

This topic provides instructions for configuring custom policies based on the predefined policies included with SiteProtector.

Important: You cannot make changes to a predefined policy.

Environments

SiteProtector provides predefined policies for the following environments:

- Windows
- Solaris
- Linux

Configuring a custom policy

Use the Policy tab to configure a custom policy.

Procedure

1. In the left pane, select the Site Node, and then click **Action** > **Manage Policy**. The Policy tab appears.
2. Select the policy, and then select **Action** > **Derive New**. The Derive New Item window appears
3. Type the name for the custom policy, and then click **OK**. The Policy Editor appears.
4. Edit the policy in the Policy Editor.
   For more information about using the Policy Editor, see the Policy Editor help.
5. Save the policy. The policy is available for you to apply to "site-level policy" agents.

Applying policy files to agents

Use the Apply Policy command to apply a customized policy file to an agent.

About this task

The information in this topic applies to the following products:

- IBM RealSecure Server Sensor
- IBM Security Network IPS G-series appliances
- SecurityFusion Module

Procedure

1. Select **Agent** from the Go to list.
2. Select the agent to which you want to apply the policy, and then click **Action** > **Apply** > **Policy**.
3. Click the **Policy** icon, and then select the Policy to apply.
4. Click the **Schedule** icon, and then schedule a job to apply the policy as follows:

If you want the job to run...	Then...
one time	1. Select **Run Once**. 2. If you want the job to start later, select the **Start** time.
on a recurring schedule	1. Select **Daily**, **Weekly**, or **Monthly**. 2. Select the time to **Start** the jobs. 3. If you want to limit the number of occurrences, select the **End by** date.

5. Click **OK**.

Applying policies to groups

This topic provides information about applying policies to a group.

Reference: For information about how to apply policies to agents of the same type but in different groups, "Applying policies with policy subscription groups" on page 61.

Assigning a policy to groups

In addition to applying policies to individual agents, you can apply policies to agents in the same group. SiteProtector provides the ability to perform the following policy assignment tasks at the group level:

- Apply the same policy to multiple agents of the same type in the same group
  For example, apply a policy to all the server sensors in a group called Server Sensors.
- Apply different policies to multiple agents of the same type in the same group
  For example, apply two different policies to the server sensors in a group called Server Sensors.
- Apply different policies to different types of agents in the same group
  For example, apply a network IPS policy and a server sensor policy to a group that contains both agents.

Applying policies to groups provides an efficient method for managing and applying policies to multiple agents in the same group. This approach does not prevent you from also applying policies to the individual agents in the group. For example, you can apply a server sensor policy to a group that contains server sensors, and then apply an additional server sensor policy to an individual server sensor in the group.

Load distribution

When you apply a policy to a group of agents, SiteProtector does not apply the policy to all agents at the same time. It divides the agents into groups and applies the policy to the groups incrementally over a period of time.

Applying policies to agents in a group

Use the Apply Policy window to apply a policy to an agent in a group.

Procedure

1. In the left pane, select the group that contains the agents, and then click **Action** > **Apply** > **Policy**. The Apply Policy window appears.

2. In the **Agent Type** list, select the type of agent that will receive the policy assignment:
   - IBM Security Network IPS G-series
   - Server Sensor
3. Click the **Policy** icon, and then select a policy from the list.
4. Perform one of the following steps:
   - To apply the policy to only agents that subscribe to the group, select the **Only apply to subscribers** check box.
   - To apply the policy to all agents in the group, clear the check box.
5. Click the **Schedule** icon, and then perform one of the following steps:
   - Select **Run Once** to apply the policy immediately.
   - Schedule a job to apply the policy.
6. Click **OK**.

Applying policies with policy subscription groups

This topic provides information about policy subscription groups and how to apply policies to agents with policy subscription groups.

What is a policy subscription group?

A *policy subscription group* is like any other group in SiteProtector except that agents subscribe to the group for their policies. The policy subscription groups acts as a central distribution center for the policy. It provides an efficient method for managing policies for a large number of agents in a central location. It also eliminates the need to apply the policy to each individual agent.

For example, 10,000 Desktop Endpoint Security agents can subscribe to a single policy subscription group for their policies. You can manage and change the policy in the policy subscription group, and all 10,000 subscriber agents will be updated at the same time.

What indicates a policy subscription group?

Policy subscription groups appear in the left pane along with all other groups. There is no visual distinction between these types of groups and other groups in the Console. For this reason, you should give policy subscription groups a name to indicate the purpose of the group, such as Policy Group for Desktop Protection Agents. The procedure for creating a policy subscription group is the same procedure for creating a regular group.

Agents

You can configure the following agents to subscribe to a policy subscription group for their policies:

- Proventia Desktop Endpoint Security agents
- IBM RealSecure Server Sensors
- IBM Security Network IPS

Example

The following example illustrates how you apply policies to agents with a policy subscription group:

- You create a group called “Policy Group for Desktop Endpoint Security Agents 8.0.”
- You deploy 10,000 Desktop Endpoint Security agents on your network.
- You define a policy for the Desktop Endpoint Security agents, and then apply it to the Policy Group for Desktop Endpoint Security Agents 8.0 group.

- You assign the Policy Group for Desktop Endpoint Security Agents 8.0 group to all 10,000 Desktop Endpoint Security agents as their policy subscription group. All 10,000 agents get their policy from this one group.

  Note: For this feature to work, all of the agents must exist in subgroups below the Policy Group for Desktop Endpoint Security Agents 8.0 group. In other words, the Policy Group for Desktop Endpoint Security Agents 8.0 group must be the parent group with policy for all of the agents. Agents cannot get their policy from a subgroup, only a parent group or the group in which they exist.
- You change the policy and reapply it to the Policy Group for Desktop Endpoint Security Agents 8.0 group. All 10,000 subscriber agents are updated simultaneously.

Rules

When you apply policies with policy subscription groups, you must follow these rules:

- The policy subscription group must be a parent group to the groups that contain the subscriber groups. Agents cannot subscribe to a subgroup for their policies.
- An agent can subscribe to only one group for its policy. An agent cannot subscribe to multiple groups for different policies. If an agent subscribes to multiple groups, then the agent gets its policy from that last group it subscribed to.
- Agents of different versions must subscribe to different groups for their custom policies. You must create two different groups, apply the different policies to the groups, and then set the different agents to subscribe to the appropriate group based on their version.
- Agents of different types can subscribe to the same group for their policies. For example, a Network IPS and a server sensor can subscribe to the same group for their policies.
- You can apply only one policy to a policy subscription group for each agent type. For example, you cannot apply two different server sensor policies to the same policy subscription group.
- In addition to the single policy that you can apply to the policy subscription group for the Desktop Protection agent, you can also apply one policy for each of the following agents:
  - IBM RealSecure Server sensor
  - IBM Security Network Intrusion Prevention System (IPS)

Assigning policy subscription groups

When you move an agent from the Ungrouped Assets folder into another group, SiteProtector attempts to set the agent's policy subscription group automatically. The success of this process depends on whether the group where you add the agent has a policy set correctly. The following table describes how SiteProtector sets the policy subscription group for agents that you manually add to other groups:

If you add the agent to a group that...	Then...
has a policy of the correct type set	SiteProtector sets this group to be the agent's policy subscription group.
does not have a policy of the correct type set	• SiteProtector searches the group hierarchy, moving up toward the top group, until it finds a group with the correct policy. • SiteProtector then sets first group it finds with a correct policy to be the agent's policy subscription group. If SiteProtector cannot find a group with the correct policy, then SiteProtector does not set the agent's policy subscription group.

Task overview

The following table describes the tasks for applying a policy to agents with a policy subscription group:

Task	Description
1	Create a group, and then define the group settings. Give the group a name to indicates its purpose, such as "Policy Group for Desktop Protection Agents." **Note:** You assign this group to the agent as the agent's policy subscription group. The agent gets its policies from this group. The group must be a parent group to the group where the agent exists.See the *IBM Security SiteProtector System Configuration Guide*.
2	Create a custom policy for the agent. See "Configuring custom policies" on page 59.
3	Apply the custom policy to the group. **Note:** SiteProtector applies the policies to any agent that subscribes to the group.See "Applying policies to groups" on page 60.
4	Assign the group to the agent as the agent's policy subscription group. **Note:** If you are applying the policy to a large number of agents, then you must assign the policy subscription group to all the agents.

Assigning a policy subscription group

Use policy subscription groups to apply common policy settings to several agents in the same group.

Procedure

1. Select a group, and then select **Agent** from the view list.
2. Select the agent, and then click **Action** > **Configure Agents** > **Assign Policy Subscription Group**.
3. Select a group in the tree.

   Important: If you select **None**, the agent will be moved outside of the grouping structure and will not inherit policies from any group.
4. Click **OK**.

Viewing policy subscription group settings

This topic describes how to view the policy subscription group setting for an agent.

Procedure

1. Select the group that contains the agent.
2. Select Agent from the **Go to** list.
3. In the right pane, locate the **Get Policy From** column.

   This column indicates the group where the agent gets its policy from. This group is the agent's policy subscription group.

Managing policy permissions at the site level

Use the Modify Policy permission to give users the ability to modify an individual site-level policy or response. The Modify Policy permission is granted for individual policies and responses only.

About this task

These procedures grant the user permission to modify the individual policy or response. The Modify Policy permission is a site-wide permission, meaning that the user can modify the policy anywhere in the site. The permission does not apply to all policies. If you want to grant a user the ability to modify

multiple policies, then you must perform this procedure for each policy. SiteProtector does not provide a global permission that allows a user to modify all policies.

Procedure

1. Select the Site node, and then click **Action** > **Manage Policy**.
2. Click the Policy or Response icon to locate the policy or response for which you want to change permissions.
3. Select the policy or response, and then click **Object** > **Properties**.
4. On the Details window, click **Permissions**.
5. In the Users and/or Groups section of the Manage Permissions window, click **Add** to add members, or **Remove** to remove members.
6. In the Select Permission Action section, select **Modify** to grant users permission to modify this policy.
7. If you want to set or change the owner of the policy, click **Advanced**, type the member name in the **Change Owner** text box, and then click **OK**.

To include...	Type this in the Change Owner box...
Local users or groups	the complete account using the following syntax: • *computer name\user name* • *computer name\group name* If you do not know the complete account information, then you must look it up using Windows Computer Management.
Domain users or groups	the complete account name using the following syntax: • *domain name\user name* • *domain name\group name* If you do not know the complete account name, then you must look it up using Check Names.

8. Click **OK**, and then click **Close** on the Details window.

Policy assignment with active directory

If you use Active Directory to populate groups with assets in SiteProtector, you might encounter issues related to policy assignments for agents. This topic describes some possible solutions for these issues.

Assets in multiple groups

When you put an asset in both an Active Directory group and a policy subscription group, and you can assign policies to both groups, the agent gets its policy based on the setting for the **Reassign agent policy based on Active Directory grouping** option. The following table describes the settings for this option:

Setting	Description
cleared	The agent continues to receive policies from the SiteProtector group.
selected	The agent receives its policy from the Active Directory group.

Moving an asset to a different Active Directory group in the same domain

The following table describes what happens if an agent subscribes to an Active Directory group for its policy, and the agent's asset is moved to a different Active Directory group on the network:

If the Active Directory information in SiteProtector is updated and the Reassign sensor policy check box is...	Then the agent...
cleared	continues to receive its policy from the original Active Directory group.
selected	receives its policy from the new Active Directory group.

Moving a computer object to a different domain in the same forest

If you move a computer object to a different domain in the same forest, what happens to the policy assigned to the original computer object depends on the Reassign sensor policy based on Active Directory grouping option, as shown in the following table:

If the Reassign sensor policy based on Active Directory grouping check box is...	Then the policy...
cleared	remains assigned to the original computer object.
selected	assignment is unpredictable, and you should remove the computer object from the old domain to resolve the ambiguity.

Moving an asset to a different domain in the same forest

The following table describes what happens if you move an asset to a different domain in the same forest, based on the method you use to move the asset:

If you...	Then...
join the computer to the new domain by renaming the domain in the computer's properties	• a new computer object is created in the new domain • the old computer object remains in the old domain • the new computer object receives a new GUID
use the Active Directory Migration Tool	• the old computer object remains in the old domain (in case you want to undo the operation) • the new computer object receives a new GUID
use the Microsoft MoveTree and Netdom utilities	• the old computer object is removed when the new computer object is created • the GUID does not change

Chapter 12. Configuring site-level responses

This chapter provides information about configuring agent responses and global responses for the following agents:

- Event Collector
- IBM RealSecure Server Sensor 6.5 and 7.0
- IBM Security Network IPS G-series appliances

Important: This section does *not* apply to the following products:

- IBM Security Network Intrusion Prevention System (IPS)
- Proventia Network Multi-Function Security (MFS)
- Proventia Server for Linux (IBM Security Server Protection)
- Proventia Server for Windows (IBM Security Server Protection)
- Proventia Desktop 8.0 (Proventia Desktop Endpoint Security) or later
- Proventia Network Anomaly Detection System (ADS)
- Proventia Network Mail Security

Reference: For step-by-step instructions about how to work with SiteProtector responses, see the *SiteProtector Help*.

Topics

What are responses?

This topic provides information about responses.

Definition

A *response* is the action that an agent takes in response to a security event. For example, when an agent performs the following actions, the agent is responding to a security event:

- The agent notifies the Console to display information about the security event.
- The agent saves the security event to the site database.
- The agent sends an email notification to a user regarding the security event.

These actions are user-defined and controlled through response settings.

Flexible responses

SiteProtector provides flexible response management and configuration options to meet your specific security and network requirements. For example, you can configure responses for the following situations:

- A single agent to send one response to the same individual security event
- A single agent to send multiple responses to the same individual security event
- Multiple agents to send the same response to the same individual security event

- Multiple agents to send different responses to the same individual security event

Required user input

When you configure responses, you must make decisions about how you want the agent to respond to the security event:

- Do you want the agent to display the security event in the Console?
- Do you want the agent to save the security event to the site database?
- Do you want the agent to send an email notification regarding the security event?
- What email address should the agent send the email to?
- How often do you want the agent to generate the response?

Your decisions determine how you should set the response options. You set some options in the response policy and other options outside of the response policy. Options set in the response policy are stored in the response file.

Global and agent responses

The following table describes the categories of responses:

Category	Description
Global	Global responses are site-wide responses that control how all agents in the entire site respond to security events. Global responses can be applied to the following agents: • IBM RealSecure Server Sensor • IBM Security Network IPS • SecurityFusion / Event Collector
Agent	Agent responses are site-level responses that control how an individual agent responds to security events. Agent responses are also version specific, meaning that the response affects only agents at a specific version. Agent responses can be applied to the following agents: • IBM RealSecure Server Sensor • IBM Security Network IPS • SecurityFusion / Event Collector **Important:** Agent responses override global responses. For example, if you apply a global response and an agent response to an agent, then the agent responds based on the agent response, not the global response.

Process

Follow this sequence when you configure responses:

1. Configure global responses.
2. Either merge the global responses with agent responses or entirely replace the agent responses with the global responses.

Supported responses by agent

The following table lists the supported response types for each agent:

Agent	Response Types
SecurityFusion / Event Collector	These responses are available for the Event Collector through the SecurityFusion Module: • Email • SNMP • User-specified
IBM Security Network IPS	These responses are available for IBM Security Network IPS: • Email • Opsec • Rskill • SNMP • User specified
IBM RealSecure Server Sensor 7.0	These responses are available for IBM RealSecure Server 7.0: • Banner • Block • Email • Fusion scripting • Rskill • SNMP • Suspend • User specified

Configuring custom agent responses

This topic describes how to configure custom agent responses from the predefined responses.

About this task

The following table describes the tasks for configuring responses to security events:

Task	Description
1	Configure a policy for the agent. In this task, you specify the *security events* that you want the agent to detect. This task requires the following procedures: • Select a policy. • Specify the events you want the agent to detect. • Save the policy. • Apply the policy to the agent. See Chapter 11, "Configuring site-level policies," on page 57
2	Customize an agent response. In this task, you specify *responses*[a] that you want the agent to generate when it detects the security events.

[a] SiteProtector provides a default response for each security event. A typical default response requires the agent to notify the Console of the security event and log the security event to the site database. The TCP reset, firewall reconfiguration, and user-defined response options are never selected in a default response.

Procedure

1. Select the Site Node, and then select **Action** > **Manage Policy**. The Policy tab appears.
2. Click the **Response** icon. The right pane lists the responses.
3. Select the response, and then click **Action** > **Derive New**. The Derive New Item window appears.
4. Type the name for the custom response, and then click **OK**. The Response Editor appears.
5. Edit the response policy as necessary with the Response Policy Editor, and then click **OK**.

Managing policy permissions at the site level

Use the Modify Policy permission to give users the ability to modify an individual site-level policy or response. The Modify Policy permission is granted for individual policies and responses only.

About this task

These procedures grant the user permission to modify the individual policy or response. The Modify Policy permission is a site-wide permission, meaning that the user can modify the policy anywhere in the site. The permission does not apply to all policies. If you want to grant a user the ability to modify multiple policies, then you must perform this procedure for each policy. SiteProtector does not provide a global permission that allows a user to modify all policies.

Procedure

1. Select the Site node, and then click **Action** > **Manage Policy**.
2. Click the Policy or Response icon to locate the policy or response for which you want to change permissions.
3. Select the policy or response, and then click **Object** > **Properties**.
4. On the Details window, click **Permissions**.
5. In the Users and/or Groups section of the Manage Permissions window, click **Add** to add members, or **Remove** to remove members.
6. In the Select Permission Action section, select **Modify** to grant users permission to modify this policy.
7. If you want to set or change the owner of the policy, click **Advanced**, type the member name in the **Change Owner** text box, and then click **OK**.

To include...	Type this in the Change Owner box...
Local users or groups	the complete account using the following syntax: • *computer name\user name* • *computer name\group name* If you do not know the complete account information, then you must look it up using Windows Computer Management.
Domain users or groups	the complete account name using the following syntax: • *domain name\user name* • *domain name\group name* If you do not know the complete account name, then you must look it up using Check Names.

8. Click **OK**, and then click **Close** on the Details window.

Part 4. Appendixes

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at

http://www.ibm.com/privacy/details/us/en sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service.”

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Index

T

U

Printed in USA