Configuring Shared Policies and Group Policies

This chapter describes how to configure and deploy shared policies to multiple sensors and how to group policies for sharing. It contains the following sections:

Configuring Shared Policies

This section describes shared policies and how to configure and deploy them. It contains the following topics:

Understanding Shared Policies

You can configure and deploy shared policies to multiple sensors. Currently only the global correlation policy can be shared. It consists of the inspection/reputation and network participation components. You can create and delete policies from any configuration pane in the IME by clicking **Add Policy** or **Delete Policy** in the upper right corner of the IME.

Shared policies are based on sensor version, not component version. You can use the current configuration of a sensor, another policy, or a template as the source for a new policy. When you use the current configuration of a sensor, the initial current configuration for the policy is taken from the sensor current configuration. When you use another policy as the basis for a new policy, the new policy is a clone of the source policy except for the new name. A template is the default configuration associated with a specified IPS version. You can select a template from any of the sensor versions managed by the IME. For example, if the IME is managing 7.0(2) and 7.0(4) sensors, you can select either of these versions, but IPS 7.0(3) is not an available selection. Only a sensor version can be used as a source template—actual sensors and existing policies may not be used.

After a policy has been created, it does not retain any connection to its source. For example, if you create a policy from a sensor configuration and that sensor configuration is later modified or even if the sensor is deleted, it has no effect on the policy.

Policy Sharing Restrictions

Pay attention to the following when configuring policy sharing:

- You can define up to ten shared policies at any given time.
- Since global correlation was introduced in IPS 7.0, only sensor versions 7.0 and later can be used as a policy source or deployment target.
- At least one sensor or policy must be configured on the IME for a policy to be created.
- Policy names must be less than 64 characters in length.
- Policy names cannot contain characters restricted by Windows (<>^*?":).
- Policy names cannot contain names restricted by Windows (con. nul. aux. prn, etc.).
- New policy names cannot match existing sensor, policy, or policy group names.
- New policy group names cannot match existing sensor or policy names.
- New sensor names cannot match existing sensor, policy, or policy group names.
- No sensor or policy can be named 'Policy Groups,' because this name uniquely identifies the Policy Group tab.

For More Information

For detailed information about global correlation, see Chapter 14, "Configuring Global Correlation."

Add Policy Field Definitions

The following fields are found in the Add Policy dialog box:

- New Policy Name—Specifies the name of the new shared policy.
- Initialize Policy From—Specifies which source you will use for the shared policy.
  - A Device Configuration—Specifies that the policy will be based on a sensor current configuration.
  - Another Policy—Specifies that the policy will be a clone of an existing policy.
  - A Version Template—Specifies that the policy will be a template of a default configuration associated with a specified IPS version.
- Select Source Sensor/Policy/Version—Specifies the sensor, policy, or version that you are choosing from which to initialize the policy.
- The New Policy Will Include These Components—Shows the global correlation components that are a part of this shared policy.

Adding and Deleting Shared Policies

To add and delete shared policies, follow these steps:

Step 1 From the IME, choose **Configuration > Add Policy**. The Add Policy dialog box appears.

Note You can configure shared policies from any configuration pane in the IME.

Step 2 In the New Policy Name field, enter a name for the new policy.

Step 3 Under Initialize Policy From, choose one of the following:

- A Device Configuration
- Another Policy
- A Version Template

Step 4 From the Select Source Sensor drop-down menu, choose the sensor, the policy, or the version that you are applying the policy to.

Step 5 Under The New Policy Will Include These Subcomponents, check the checkboxes of the global correlation components you want to include, and the click **OK**. A tab with the new policy name appears.

Step 6 Select the new policy tab and configure inspection/reputation and network reputation.

Step 7 To delete a shared policy, select the policy tab that you want to delete and click **Delete Policy**. The Delete Policy dialog box appears asking if you are sure you want to delete this policy. Click **Yes** to delete it. The tab is deleted.

For More Information

For detailed information about global correlation, see Chapter 14, "Configuring Global Correlation."

Deploying Shared Policies

To deploy shared policies, follow these steps:

Step 1 From the IME, choose **Configuration >** *shared_policy_name* **> Deployment > Deployment Management > deployment**.

Step 2 Under Select From the Following Sensors and Policy Groups for Deployment, check the checkboxes for the sensors and policy groups that you want to deploy.

Step 3 Under Select From the Following Components for Deployment, since there is currently only one shared policy, global correlation, you accept both inspection/reputation and network participation, or uncheck one of those components and just use one.

Step 4 Click **Apply** and then **Deploy**. The Policy Deployment Results dialog box appears stating the results of the deployment and displays reasons for successful or unsuccessful deployment.

Note If the configuration on the sensor is different than the policy being deployed, you receive a warning that the configuration will be overwritten. You must click **OK** for deployment to proceed. If you do not want to receive this message again, you can disable it in **Tools > Policy Deploy Warning**. If the configuration on the sensor is the same as the policy, the policy is not deployed, and you receive no warning.

For More Information

For detailed information about global correlation, see Chapter 14, "Configuring Global Correlation."

Configuring Policy Groups

You can group multiple sensors for shared policy deployment. Policy groups are only used for shared policy deployment. You create a tree hierarchy of named groups. When you add a sensor to the IME, it is immediately available for insertion into the policy group tree. When you remove a sensor in a group from the IME, it remains in the policy group until you remove it manually. However, no deployment for that sensor can occur until you add it again to the IME.

Pay attention to the following when creating policy groups:

- A group can contain child groups and sensors, but sensors cannot contain children.
- A group or sensor node can only have one parent.
- A group name cannot match any sensor name.
- No matter how many times a sensor happens to appear in various deployed groups, at most one deployment to that sensor can happen.

To manage group policies, follow these steps:

Step 1 From the IME, choose **Configuration > Policy Groups > Group Management > Groups**.

Step 2 Click **Add Group** to add a new group, and in the Enter New Group Name field, enter a name for the new group.

Step 3 Select the new group name and click **Add Sensors** to add sensors to this policy group, The Add Sensors dialog box appears.

Step 4 Under Select From the Following Sensors, check the checkboxes of the sensor(s) you want to include, and then click **OK**. The selected sensor(s) appear under the new policy group.

Step 5 To copy a policy group, select it, click **Copy**, and then click **Paste**. The copied policy group and sensor(s) appear under the selected policy group.

Step 6 To rename a policy group, select it, and then click **Rename**. The Rename Group dialog box appears.

Step 7 In the Enter New Group Name field, enter the new name.

Step 8 To delete a policy group, select it, and then click **Delete**. The policy group is immediately deleted.

Step 9 Click **Move Up** and **Move Down** to rearrange items in the Policy Groups tree.

Step 10 To save your changes, click **Apply**.