

Configuring a Secure Application Manager Resource Policy (NSM Procedure)

When you enable the secure application manager access feature for a role, you need to create resource policies that specify which application servers a user may access. These policies apply to both the Java version and the Windows version of the Secure Application Manager (JSAM and WSAM, respectively). When a user makes a request to an application server, the Secure Access device evaluates the SAM resource policies. If the Secure Access device matches a user's request to a resource listed in a SAM policy, the Secure Access device performs the action specified for the resource.

To configure Secure Application Manager resource policy:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure a Secure Application Manager resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > SAM**.
3. Add or modify settings as specified in Table 1.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Secure Application Manager Resource Policy Configuration Details

Option	Function	Your Action
Access Control > General tab		
Name	Specifies the name for the policy.	Enter the name.
Description	Describes the policy.	Enter a description.
New Resources	Specifies the servers to which this policy applies.	Enter the server path.
Applies to roles	Specifies the roles to which this policy applies.	Select one of the following options from the drop-down list: <ul style="list-style-type: none">■ All—Applies the policy to all users.■ Selected—Applies the policy only to users who are mapped to roles in the Role Selection section.■ Except those selected—Specifies one or more detailed rules for this policy.

Table 1: Secure Application Manager Resource Policy Configuration Details (continued)

Option	Function	Your Action
Action	Allows or denies access to the servers specified in the resources list.	<p>Select one of the following options from the drop-down list.</p> <ul style="list-style-type: none"> ■ Allow socket access—Allows access to the application servers specified in the Resources list. ■ Deny socket access—Denies access to the servers specified in the Resources list. ■ Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Role Selections tab		
Role Selections	<p>Maps roles to access resources.</p> <p>NOTE: This tab is enabled only when you select selected or Except those selected from the Applies to the role drop-down list.</p>	Select a role and click Add to add roles from Non-members to Members list.
Detailed Rules tab		
Name	<p>Specifies the detailed rule name.</p> <p>NOTE: The Detailed Rules tab is displayed only when you select the Detailed Rules option from the Action drop-down list.</p>	Enter a name.
Action	Specifies the action you want to perform if the user request matches a resource in the resource list (optional).	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Allow socket access—Allows the user to access the resource. ■ Deny socket access—Denies the user to access the resource.
New Resources	Specifies the resource to which detailed rule applies.	<p>Specify any one of the following:</p> <ul style="list-style-type: none"> ■ The same or a partial list of the resources specified on the General tab. ■ A specific path or file on the server(s) specified on the General tab, using wildcards when appropriate. ■ A file type, preceded by a path if appropriate or just specify <code>*/*.file_extension</code> to indicate files with the specified extension within any path on the server(s) specified on the General tab.

Table 1: Secure Application Manager Resource Policy Configuration Details (continued)

Option	Function	Your Action
Conditions	Specifies one or more expressions to evaluate to perform the action.	Specify one of the following options: <ul style="list-style-type: none">■ Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators.■ Custom expressions: Using the custom expression syntax, write one or more custom expressions.
Options		
IP based matching for Hostname based policy resources	Secure Access device compares the IP to its cached list of IP addresses to determine if a host name matches an IP address. If there is a match, then the Secure Access device accepts the match as a policy match and applies the action specified for the resource policy.	Select Options > IP based matching for Hostname based policy resources option to enable this feature.

- Related Topics**
- Configuring a Telnet and Secure Shell Resource Policy (NSM Procedure)
 - Configuring a Terminal Service Resource Policy (NSM Procedure)

Published: 2009-08-20