

Configuring a File Rewriting Resource Policy (NSM Procedure)

File rewriting resource policies specify which Windows resources a user may access, as well as the encoding to use when communicating with Windows and NFS file shares. When a user makes a file request, the Secure Access device evaluates the resource policies corresponding to the request, such as Windows access resource policies for a request to fetch an MS Word document (.doc file). After matching a user's request to a resource listed in a relevant policy, the Secure Access device performs the action specified for the resource.

To configure a file rewriting 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 file rewriting resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Files**.
3. Select a policy, and then enter the name, the description, and the resources for the policy.
4. In the Applies to roles list. Select one:
 - **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**—Applies this policy to all users except for those who map to the roles in the Role Selection section.
5. Select the role, and click **Add** to move the roles from non-members to members list.



NOTE: The Role Selections tab is enabled only when you select **Selected** or **Except those selected** option from the Applies to roles drop-down list.

6. Enter the name, and specify the resources for the detailed rules.



NOTE: The Detailed Rules tab is enabled only when you select the **Detailed Rules** option from the Action drop-down list.



NOTE: To apply detailed rules to the roles, see Step 4.

7. Specify one or more expressions in the Conditions box to evaluate in order to perform the action.
8. To specify actions and additional settings on the file rewriting policy using Table 1 on page 2.
9. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 1: Configuring File Rewriting Resource Policies Details

Option	Function	Your Action
Windows ACL > General tab		
Action	Specifies the action to access resources.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Allow—Allows access to the resources specified in the Members list. ■ Deny—Denies access to the resources specified in the Members list. ■ Detailed Rules—Allows you to specify one or more detailed rules for this policy.
Read-only	Prevents users from saving files on the server. NOTE: This box displays only if you select Allow in the Action drop-down list.	Select the Read-only check box to enable this feature.
Windows ACL > Detailed Rules tab		
Action	Specifies the action to perform if the user request matches a resource in the Resources list.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Allow—Allows the user access to the resource. ■ Deny—Denies the user access to the resource.
Read-only	Prevents users from saving files on the server. NOTE: This box is enabled only when you select Allow from the Action drop-down list.	Select the Read-only check box to enable this feature.
Windows SSO > General tab		

Table 1: Configuring File Rewriting Resource Policies Details (continued)

Option	Function	Your Action
Action	<p>Specifies the action to take when a resource requires credentials.</p>	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Use Specified Credentials(Variable Password)...—Secure Access device uses specified credentials with variable password to pass to the Windows share or directory ■ Use Specified Credentials(Fixed Password)...—Secure Access device uses specified credentials with fixed password to pass to the Windows share or directory. ■ Prompt for user credentials—Secure Access device intermediates the share challenge by presenting an authentication challenge in the Secure Access device the first time a user attempts to access the share. ■ Detailed Rules—Specifies one or more detailed rules for this policy.
Username	<p>Specifies a username to submit to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials(Variable Password)... or Use Specified Credential(Fixed Password)... options from the Action drop-down list.</p>	<p>Enter a variable. For example enter <USERNAME> or a static username. For example, administrator to submit to the Windows share or directory.</p> <p>NOTE: When entering a variable, you may also include a domain. For example enter yourcompany.net<USERNAME></p>
Variable Password	<p>Specifies a variable password to Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials(Variable Password)... option from the Action drop-down list.</p>	<p>Enter the variable password.</p>

Table 1: Configuring File Rewriting Resource Policies Details (continued)

Option	Function	Your Action
Fixed Password	<p>Specifies a static password to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credential(Fixed Password)... option from the Action drop-down list.</p>	Enter the static password.
Windows SSO > Detailed Rules tab		
Action	Specifies the action to take when a resource requires credentials.	<p>Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> ■ Use System Credentials...—Secure Access device submits the stored credentials to resources. ■ Use Specified Credentials(Variable Password)...—Secure Access device uses specified credentials with variable password to pass to the Windows share or directory ■ Use Specified Credentials(Fixed Password)...—Secure Access device uses specified credentials with fixed password to pass to the Windows share or directory. ■ Prompt for user credentials—Secure Access device intermediates the share challenge by presenting an authentication challenge in the Secure Access device the first time a user attempts to access the share. ■ Detailed Rules—Specifies one or more detailed rules for this policy.

Table 1: Configuring File Rewriting Resource Policies Details (continued)

Option	Function	Your Action
Username	<p>Specifies a username to submit to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials(Variable Password)... or Use Specified Credential(Fixed Password)... options from the Action drop-down list.</p>	<p>Enter a variable. For example enter <USERNAME> or a static username. For example enter administrator to submit to the Windows share or directory.</p> <p>NOTE: When entering a variable, you may also include a domain. For example enter yourcompany.net\<USERNAME></p>
Variable Password	<p>Specifies a variable password to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credentials(Variable Password)... option from the Action drop-down list.</p>	<p>Enter the variable password.</p>
Fixed Password	<p>Specifies a static password to the Windows share or directory.</p> <p>NOTE: This box is enabled only when you select the Use Specified Credential(Fixed Password)... option from the Action drop-down list.</p>	<p>Enter the static password.</p>
Windows Compression		
Action	<p>Specifies the action you want to perform to allows or deny access to the resources.</p>	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Compress—Secure Access device compresses the supported content types from the specified resource. ■ Do not compress—Secure Access device does not compress the supported content types from the specified resource. ■ Use Detailed Rules—Specifies one or more detailed rules for this policy.

Table 1: Configuring File Rewriting Resource Policies Details (continued)

Option	Function	Your Action
File Policy 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 the IP based matching for Hostname based policy resources check box to enable this feature.
Case sensitive matching for the path component in File resources	Requires users to enter a case-sensitive path component.	Select the Case sensitive matching for the path component in File resources check box to enable this feature.
Encoding	Specifies the encoding to use when communicating with Windows and NFS file shares.	Select from the drop-down list.
NTLM Version	Specifies NTLM for file share authentication.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ NTLM v1—Uses only NTLM V1 for file share authentication. ■ NTLM v2—Uses only NTLM V2 for file share authentication.
Number of NTLM authentication protocol variant attempts	Controls the number of login attempts while doing SSO.	Select either High or Low .

- Related Topics**
- Configuring SAML SSO Artifact Profile Resource Policy (NSM Procedure)
 - Configuring a SAML Access Control Resource Policy (NSM Procedure)