

Configuring Secure Access Role Mapping Rules (NSM Procedure)

Role mapping rules are conditions a user must meet for the device to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

To configure role mapping rules for an administrator/user realm:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure role mapping rules for an administrator/user realm.
3. Click the **Configuration** tab and select either **Administrators > Admin Realms** or **Users > User Realms**. The corresponding workspace appears.
4. Click the **New** button. The New dialog box appears.
5. Configure role mapping rules for an administrator/user realm using the settings described in Table 1 on page 1.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Role Mapping Rules Configuration Details

Option	Function	Your Action
Role Mapping Rules tab		
User must select from among assigned roles	Specifies if you want the users to select from the assigned roles.	Select Admin Realm > Role Mapping Rules > User must select from among assigned roles to enable this option.
User must select the sets of merged roles assigned by each rule	Specifies if you want users to select the sets of merged roles that are assigned by each rule.	Select Admin Realm > Role Mapping Rules > User must select the sets of merged roles assigned by each rule to enable this option.
Role Mapping Rules > New > Settings tab		
Name	Specifies the name entered on the sign-in page.	Enter a name.
Assign these roles if the rule matches > Non-members	Specifies the list of non-members whose roles are not matched with the rules.	Select a non-member from the list to assign to the authenticated user by adding/removing it to/from the Members list.
Stop processing rules when this rule matches	Specifies if you want the device to stop evaluating role mapping rules if the user meets the conditions specified for this rule.	Select Admin Realms > Role Mapping Rules > Settings > Stop processing rules when this rule matches to enable this option.

Table 1: Role Mapping Rules Configuration Details (continued)

Option	Function	Your Action
Role mapping rule type	Specifies the type of role mapping rule.	Select the type of role mapping rule from the drop-down list.
is/is not NOTE: This option is enabled only if you select either if username or if certificate has any of the attributes as the role mapping rule type.	Specifies the conditional expression used in the rule.	Select an option from the drop-down list.
New	Specifies the rules that are used for matching.	Enter the respective rule matching entries. NOTE: <ul style="list-style-type: none">■ Enter a new username if you select if username as role mapping rule type.■ Enter a new expression if you select if user has any of these custom expressions as role mapping rule type.■ Enter a new value if you select if certificate has any of the attributes as role mapping rule type.
Attribute	Specifies the role mapping role attributes. NOTE: This option is enabled only if you select if certificate has any of the attributes as the role mapping rule type.	Enter an attribute name.

- Related Topics**
- Configuring Secure Access Sign-In Policies (NSM Procedure)
 - Configuring Secure Access Authentication Policies (NSM Procedure)