

## Configuring Secure Access Authentication Realms (NSM Procedure)

An authentication realm specifies the conditions that users must meet to sign into the Secure Access device.

To configure an authentication realm:

1. In the NSM 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 authentication realms.
2. Click the **Configuration** tab, select **Administrators > Admin Realms** or **Users > User Realms**. The corresponding workspace appears.
3. Click the **New** button. The New dialog box appears.
4. Configure the server using the settings described in Table 1 on page 1.
5. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 1: Secure Access Authentication Realms Configuration Details**

Option	Function	Your Action
<b>General tab</b>		
Realm Name	Specifies the name of the realm.	Enter a name.
Description	Describes the realm.	Enter a description.
When editing, start on the Role Mapping page	Specifies that the Role Mapping tab is selected when you open the realm for editing.	Select <b>General &gt; When editing, start on the Role Mapping page</b> to enable this option.
Authentication	Specifies an authentication server to use for authenticating users who sign in to this realm.	Select an authentication server from the drop-down list.
Directory/Attribute	Specifies a directory/attribute server to use for retrieving user attribute and group information for role mapping rules and resource policies.	Select a directory/attribute server from the drop-down list (optional).
Accounting	Specifies a RADIUS accounting server to use to track when a user signs in and out of the Secure Access device.	Select a RADIUS accounting server from the drop-down list (optional).

**Table 1: Secure Access Authentication Realms Configuration Details** (continued)

Option	Function	Your Action
Additional Authentication Server	Specifies the name of the secondary authentication server to submit secondary user credentials to an SSO-enabled resource or enable two-factor authentication to access the Secure Access device.  <b>NOTE:</b> You cannot choose an anonymous server, certificate server, or eTrust SiteMinder server.	Select a secondary authentication server from the drop-down list.
End session if authentication against this server fails	Controls access to the Secure Access device based on the successful authentication of the user's secondary credentials. If selected, authentication fails if the user's secondary credentials fail.	Select <b>General &gt; End session if authentication against this server fails</b> to enable this option.
Username for Secondary Auth	Specifies the username of the secondary authentication server.	Select the mode of submission of username to the secondary authentication server from the drop-down list:  <ul style="list-style-type: none"> <li>■ <b>Username is specified by user on sign-in page</b>—Prompts the user to manually submit his username to the secondary server during the Secure Access device sign-in process.</li> <li>■ <b>Predefined user name template</b>—Automatically submits a username to the secondary server during the Secure Access device sign-in process.</li> </ul>
Predefined User Name	Specifies the predefined username.	Enter static text or a valid variable.
Password for Secondary Auth	Specifies the password for the secondary authentication server.	Select the mode of submission of password to the secondary authentication server from the drop-down list:  <ul style="list-style-type: none"> <li>■ <b>Username is specified by user on sign-in page</b>—Prompts the user to manually submit his password to the secondary server during the Secure Access device sign-in process.</li> <li>■ <b>Predefined user name template</b>—Automatically submits a password to the secondary server during the Secure Access device sign-in process.</li> </ul>

**Table 1: Secure Access Authentication Realms Configuration Details** (continued)

Option	Function	Your Action
Predefined Password	Specifies the predefined password.	Enter static text or a valid variable.
Enable Dynamic policy evaluation	Uses dynamic policy evaluation for this realm.	Select <b>General &gt; Enable Dynamic policy evaluation</b> to enable an automatic timer for dynamic policy evaluation of this realm's authentication policy, role mapping rules, and role restrictions.
Refresh roles	Refreshes the roles of all users in this realm. (This option does not control the scope of the Refresh Now button.)	Select <b>General &gt; Refresh roles</b> to enable this option.
Refresh policies	Refreshes the resource policies (not including Meeting and Email Client) for all users in this realm. (This option does not control the scope of the Refresh Now button.)	Select <b>General &gt; Refresh policies</b> to enable this option.
Refresh interval (minutes)	Specifies how often you want the Secure Access device to perform an automatic policy evaluation of all currently signed-in realm users.	Enter the number of minutes (5 to 1440).

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

