

Configuring Secure Access Sign-In Policies (NSM Procedure)

You can create sign-in policies to define URLs that you can use to access the Secure Access device. There are two types of sign-in policies—one for users and one for administrators. When configuring sign-in policies, you must associate realms, sign-in pages, and URLs.

To configure sign-in policies, you must follow these procedures:

1. Creating Authorization-Only Policies on page 1
2. Creating User/Administrator URLs on page 2
3. Creating Meeting URLs on page 3

Creating Authorization-Only Policies

The authorization-only policy is similar to a reverse proxy. Typically, a reverse proxy is a proxy server that is installed in front of the Web Servers.

With an authorization-only policy, you select a user role. The device acts as a reverse proxy server and performs authorization against the Netegrity SiteMinder server for each request.

To configure an authorization-only policy:

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 an authorization-only policy.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Policies > Authorization-Only Policies**. The corresponding workspace appears.
3. Add or modify settings on the authorization-only policy as specified in Table 1 on page 1.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Authorization-Only Policy Configuration Details

Option	Function	Your Action
Virtual Hostname	Accesses the backend application and sends the request to the original requesting Web browser.	Enter a valid name that maps to the device's IP address. NOTE: The name must be unique among all the virtual hostnames used in pass-through proxy's hostname mode. Also, do not include the protocol (for example, http:) in this option.

Table 1: Authorization-Only Policy Configuration Details (continued)

Option	Function	Your Action
Backend URL	Allows the client to redirect to this URL. The request from the virtual hostname gets transformed as a request to this URL.	Enter a valid URL for the remote server. NOTE: You must specify the protocol, hostname, and port of the server. For example, enter <code>http://www.mydomain.com:8080/*</code> .
Description	Specifies the description of the policy.	Enter a description for the policy.
Authorization Server	Specifies the Netegrity SiteMinder server that manages user authentication and access.	Select the corresponding Netegrity SiteMinder server.
Role Option	Specifies the user role.	Select one of the user role options. NOTE: Only the following user role options are applicable for authorization-only policies. <ul style="list-style-type: none">■ Allow browsing un-trusted SSL (Users > User Roles > RoleName > Web > Options).■ HTTP connection timeout (Users > User Roles > RoleName > Web > Options).■ Source IP restrictions (Users > User Roles > RoleName > General > Restrictions).■ Browser restrictions (Users > User Roles > RoleName > General > Restrictions).
Enable	Enables or disables the individual policy.	Select Authorization-Only Policies > Enable to enable this option.

Creating User/Administrator URLs

To configure a user or administrator URL:

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 a user/administrator URL.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Policies > User/Administrator URLs**. The corresponding workspace appears.
3. Add or modify settings on the user/administrator URL as specified in Table 2 on page 3.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 2: User/Administrator URLs Configuration Details

Option	Function	Your Action
General tab		
Sign-in URL	Specifies the sign-in URL.	Enter a valid URL for the sign-in URL.
Description	Specifies the description of the user/administrator URL policy.	Enter a description for the user/administrator URL policy.
Enable	Enables or disables the individual policy.	Select User/Administrator URLs > Enable to enable this option.
Sign-in Page	Specifies the customized properties in the end-user's welcome page such as the welcome text, help text, logo, header, and footer.	Select the sign-in page from the drop-down list.
Realm Select	Specifies the type of the realm that you want to choose.	Select the realm select from the drop-down list.
Administrator > Selected Admin Realms > Non-members	Moves the selected admin realms from non-members to members.	Select the admin realms from Non-members to Members.
User > Meeting URL	Specifies the URL that controls the sign-in page, which you can view when you sign into a meeting on the Secure Access device.	Select the meeting URL from the drop-down list.
User > Selected User Realms > Non-members	Moves the selected user realms from non-members to members.	Select the user realms from Non-members to Members.

Creating Meeting URLs

To configure a meeting URL:

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 a meeting URL.
2. Click the **Configuration** tab, and select **Authentication > Signing In > Sign-in Policies > Meeting URLs**. The corresponding workspace appears.
3. Add or modify settings on the meeting URL as specified in Table 3 on page 4.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 3: Meeting URLs Configuration Details

Option	Function	Your Action
User Type	Specifies the type of sign-in policy.	Select the type of policy from the drop-down list (for example, enter Meeting).
Sign-in URL	Specifies the URL that you want to associate with the meeting URL policy.	Enter a valid URL. NOTE: Use the format <host>/<path> where <host> is the hostname of the device and <path> is any string that you enter.
Description	Describes of the meeting URL policy.	Enter a description of the meeting URL policy.
Enable	Enables or disables the individual policy.	Select Meeting URLs > Enable to enable this option.
Sign-in Page	Specifies the meeting sign-in page.	Select a meeting sign-in page from the drop-down list.

- Related Topics**
- Configuring Secure Access Sign-In Pages (NSM Procedure)
 - Configuring a SAML Access Control Resource Policy (NSM Procedure)