

Creating and Configuring Secure Access Device Administrator Roles (NSM Procedure)

An administrator role specifies Secure Access device management functions and session properties for administrators who map to the role. You can customize an administrator role by selecting the Secure Access device feature sets and user roles that members of the administrator role are allowed to view and manage. You can create and configure administrator roles through the Delegated Admin Roles page.



NOTE: To create individual administrator accounts, you must add the users through the appropriate authentication server (not the role). For example, to create an individual administrator account, you may use settings in the **Authentication > Auth. Servers > Administrators > Users** page of the admin console.

To create an administrator role:

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 administrator role.
2. Click the **Configuration** tree tab, and select **Administrators > Admin Roles**.
3. Click the **New** button and the New dialog box appears.
4. Click **General > Overview** to add or modify settings as specified in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Administrator Role Configuration Details

Option	Function	Your Action
General > Overview tab		
Name	Specifies a unique name for the administrator role.	Enter a name.
Description	Describes the administrator role.	Enter a brief description for the administrator role.
Session Options	Specifies the maximum session length, roaming capabilities, and session persistence.	Select General > Session Options to apply the settings to the role.
UI Options	Specifies customized settings for the Secure Access device welcome page for Odyssey Access Client users mapped to this role.	Select General > UI Options to apply the settings to the role.

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Delegated Users Settings > Roles > Delegate User Roles		
Administrators can manage ALL roles	Specifies whether the administrator can manage all roles.	Select the user roles in the Non-members list and click Add if you only want to allow the administrator role to manage selected user roles
Access	Specifies which user role pages the delegated administrator can manage.	Select an access option from the drop-down list. <ul style="list-style-type: none"> ■ Select Write All to specify that members of the administrator role can modify all user role pages. ■ Select Custom Settings to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user role pages.
Delegated Users Settings > Roles > Delegate As Read-Only Role		
Administrator can view (but not modify) ALL roles	Allows the administrator to view the user roles, but not manage.	Select the user role that you want to allow the administrator to view. <p>NOTE: If you specify both write access and read-only access for a feature, the Secure Access device grants the most permissive access.</p>
Delegated Users Settings > Realms > Delegate User Realms		
Administrator can manage ALL realms	Specifies whether the administrator can manage all user authentication realms.	Select the user realm. If you only want to allow the administrator role to manage selected realms, select those realms in the Members list and click Add .

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Access	Specifies which user authentication realms pages that the delegated administrator can manage.	<p>Select an access option from drop-down list.</p> <ul style="list-style-type: none"> ■ Select Write All to specify that members of the administrator role can modify all user authentication realm pages. ■ Select Custom Settings to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user authentication realm pages.
Delegated Users Settings > Realms > Delegate As Read-Only Realms		
Administrator can view (but not modify) ALL realms	Allows the administrator to view the user authentication realms, but not modify.	<p>Select the user authentication realms that you want to allow the administrator to view.</p> <p>NOTE: If you specify both write access and read-only access for an authentication realm page, the Secure Access device grants the most permissive access.</p>
Delegated Administrator Settings > Management of Admin roles		
Manage ALL admin roles	Manages all admin roles.	Select Delegated Administrator Settings > Management of Admin roles > Manage ALL admin roles to manage all the admin roles.
Allow Add/Delete admin roles	<p>Allows the security administrator to create administrator roles, even if the security administrator is not part of the Administrators role.</p> <p>NOTE: This option appears only when you enable the Manage All admin roles option.</p>	Select to allow the security administrator to add and delete admin roles.

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Access	<p>Indicates the level of access that you want to allow the security administrator role to set for system administrators.</p> <p>NOTE: This option appears only when you enable the Manage All admin roles option.</p>	<p>Select an access option:</p> <ul style="list-style-type: none"> ■ Deny All—Specifies that members of the security administrator role cannot see or modify any settings in the category. ■ Read All—Specifies that members of the security administrator role can view, but not modify, all settings in the category. ■ Write All—Specifies that members of the security administrator role can modify all settings in the category. ■ Custom Settings—Allows you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.
Delegated Administrator Settings > Management of Admin realms		
Manage ALL admin realms	Manages all admin realms.	Select Delegated Administrator Settings > Management of Admin realms > Manage ALL admin realms .
Allow Add/Delete admin realms	<p>Allows the security administrator to create and delete administrator realms, even if the security administrator is not part of the administrators role.</p> <p>NOTE: This option only appears when you choose to enable the Manage All admin realms.</p>	Select to allow the security administrator to add and delete admin realms.

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Access	<p>Indicates the level of realm access that you want to allow the security administrator role to set for system administrators for each major set of admin console pages.</p> <p>NOTE: This option appears only when you enable the Manage All admin realm option.</p>	<p>Select an access option:</p> <ul style="list-style-type: none"> ■ Deny All—Specifies that members of the security administrator role cannot see or modify any settings in the category. ■ Read All—Specifies that members of the security administrator role can view, but not modify, all settings in the category. ■ Select Write All—Specifies that members of the security administrator role can modify all settings in the category. ■ Select Custom Settings—Allows you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.
Delegated Resource Policies > All tab		

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Access	Indicates the level of access that you want to allow the administrator role for each Resource Policies submenu.	Select an access option: <ul style="list-style-type: none"> ■ Deny All—Specifies that members of the administrator role cannot see or modify any resource policies. ■ Read All—Specifies that members of the administrator role can view, but not modify, all resource policies. ■ Write All—Specifies that members of the administrator role can modify all resource policies. ■ Custom Settings—Allows you to pick and choose administrator privileges (Deny, Read, or Write) for each type of resource policy or for individual resource policies. <p>NOTE: The Web, File, SAM, Telnet SSH, Terminal Services, Network Connect, and Email Client tabs are enabled only when you select Custom Settings from the drop down list.</p>
Delegated Resource Policies > Web > File > SAM > Telnet SSH > Terminal Services > Network Connect		
Access	Allows you to pick and choose administrator privileges for each type of resource policy.	Select Deny or Read or Write access level for the type of resource.
Additional Access Policies	Allows you to specify access level to individual policy (For example, if you want to control access to a resource policy that controls access to www.google.com)	Select a resource policy.
Access	Allows you to pick and choose administrator privileges for each individual resource policy.	Select Read or Write access level for the policy.
Delegated Resource Policies > Email Client		

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Access	Allows you to pick and choose administrator privileges (Deny, Read, or Write) for the policy.	Select Deny or Read or Write access level for the.
Delegated Resource Profiles > All tab		
Access	Indicate the level of access that you want to allow the administrator role for each Resource Profiles.	Select an access option: <ul style="list-style-type: none"> ■ Deny All—Specifies that members of the security administrator role cannot see or modify any settings in the category. ■ Read All—Specifies that members of the security administrator role can view, but not modify, all settings in the category. ■ Write All—Specifies that members of the security administrator role can modify all settings in the category. ■ Custom Settings—Allows you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category. <p>NOTE: The Web, File, SAM, Telnet SSH, and Terminal Services tabs are enabled only when you select Custom Settings from the drop down list.</p>
Delegated Resource Profiles > Web > File > SAM > Telnet SSH > Terminal Services		
Access	Allows you to pick and choose administrator privileges for each type of resource profiles.	Select Deny or Read or Write access level for the type of resource.
Additional Access Profiles	Allows you to specify access level to individual profiles (For example, if you want to control access to a resource profiles that controls access to www.google.com).	Select the resource profile for which you want to provide a custom access level, and click Add .

Table 1: Administrator Role Configuration Details (continued)

Option	Function	Your Action
Access	Allows you to pick and choose administrator privileges (Deny, Read, or Write) for the profiles.	Select Read or Write access level for the profiles.

- Related Topics**
- Configuring Access Options using Remote Access Mechanisms Overview
 - Configuring Secure Access General Session Options (NSM Procedure)
 - Creating and Applying a Secure Access Device Template
 - Verifying Imported Device Configurations