

## Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure)

An administrator role defines administrator session and personalization settings. You can create and configure an administrator role from the Infranet Controller configuration tree.

To create an administrator role:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure administrator role.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators > Admin Roles**.
4. Add or modify settings on the **Admin Role** tab as specified in Table 1.
5. Click one:
  - **OK** — Saves the changes.
  - **Cancel** — Cancels the modifications.



**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, select **Authentication > Auth. Servers > Administrators > Users** from the NSM UI.

**Table 1: Administrator Role Configuration Details**

Option	Function	Your Action
<b>Admin Role &gt; General tab</b>		
Name	Specifies a unique name for the administrator role.	Enter a name.
<b>Admin Role &gt; General &gt; Overview tab</b>		
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 <b>General &gt; Session Options</b> to apply the settings to the role.
UI Options	Specifies the logo, color, navigation menus and the copyright notice.	Select <b>General &gt; UI Options</b> to apply the settings to the role.
<b>Admin Role &gt; General &gt; Restrictions &gt; Source IP Restrictions tab</b>		

**Table 1: Administrator Role Configuration Details** (continued)

Option	Function	Your Action
Allow	Specifies from which IP addresses users can access an Infranet Controller sign-in page, be mapped to a role, or access a resource.	<ul style="list-style-type: none"> <li>■ Select <b>Users from any IP address</b> to enable users to sign into the Infranet Controller from any IP address in order to satisfy the access management requirement.</li> <li>■ Select <b>Users from IP addresses which pass the specifies matching policies</b> to allow you to specify user access to the listed IP addresses.</li> </ul>
Source IP Address	Specifies the source IP addresses.	Enter the IP address.
Source IP Netmask	Specifies the IP netmask.	Enter the IP netmask.
Access	Specifies whether to allow or deny access.	<ul style="list-style-type: none"> <li>■ Select <b>Allow</b> to allow the user to use the IP.</li> <li>■ Select <b>Deny</b> to prevent users from using the IP.</li> </ul>
<b>Admin Role &gt; General &gt; Restrictions &gt; Browser Restrictions tab</b>		
Allow	Specifies from which web browsers users can access an Infranet Controller sign-in page or be mapped to a role.	<ul style="list-style-type: none"> <li>■ Select <b>Browsers with any user-agent</b> to allow users to access the Infranet Controller or resources using any of the supported Web browsers.</li> <li>■ Select <b>Browsers whose user-agent pass the matching policies defined below</b> to allow you to define browser access control rules.</li> </ul>
User agent pattern	Specifies the format.	<p>Enter a string in the format</p> <p>* &lt; browser_string &gt; *</p> <p>where start (*) is an optional character used to match any character and &lt; browser_string &gt; is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser.</p> <p><b>NOTE:</b> You cannot include escape characters (\) in browser restrictions.</p>
Action	Specifies whether to allow or deny access.	<ul style="list-style-type: none"> <li>■ Select <b>Allow access</b> to allow users to use a browser that has a user-agent header containing the &lt; browser_string &gt; substring.</li> <li>■ Select <b>Deny access</b> to prevent users from using a browser that has a user-agent header containing the &lt; browser_string &gt; substring.</li> </ul>

**Table 1: Administrator Role Configuration Details** (continued)

Option	Function	Your Action
<b>Admin Role &gt; General &gt; Restrictions &gt; Certificate Restrictions tab</b>		
Allow	Restricts Infranet Controller and resource access by requiring client-side certificates	<ul style="list-style-type: none"> <li>■ Select <b>All users</b> to allow users to access the Infranet Controller or resources from any machine.</li> <li>■ Select <b>Users with a trusted client certificate</b> to allow users to access the Infranet Controller from a machine with a trusted client certificate.</li> </ul>
Certificate Field	Specifies the certificate field.	Enter the certificate field.
Expected Value	Specifies the expected value.	Enter the expected value.
<b>Admin Role &gt; General &gt; Restrictions &gt; Host Checker Restrictions tab</b>		
Enforce	Specifies the Host Checker policy at the role level.	<ul style="list-style-type: none"> <li>■ Select <b>Allow all users</b> to restrict Host Checker to be installed in order for the user to meet the access requirement.</li> <li>■ Select <b>Allow users whose workstations meet the requirements specified by the Host Checker policies</b> to requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement.</li> </ul>
Host Checker policies	Specifies the Host Checker policies.	Select the required Host Checker policies.
Allow access to the role if	Specifies access to the role	<ul style="list-style-type: none"> <li>■ Select <b>All of the selected policies pass</b> to allow access only if all the policy requirements are met.</li> <li>■ Select <b>Any ONE of the selected policies pass</b> to allow access even if one policy requirement is met.</li> </ul>
<b>Admin Role &gt; General &gt; Users &gt; Roles &gt; Delegate User Roles</b>		
Administrators can manage ALL roles	Specifies whether the administrator can manage all roles	Select the user roles. If you only want to allow the administrator role to manage selected user roles, select those roles in the Non-members list and click <b>Add</b> to move it to the Members list.
Access	Specifies which user role pages the delegated administrator can manage.	<ul style="list-style-type: none"> <li>■ Select <b>Write All</b> to specify that members of the administrator role can modify all user role pages.</li> <li>■ Select <b>Custom Settings</b> to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user role pages.</li> </ul>
<b>Admin Role &gt; General &gt; Users &gt; Role &gt; Delegate As Read-Only Role</b>		

**Table 1: Administrator Role Configuration Details** (continued)

Option	Function	Your Action
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.  <b>NOTE:</b> If you specify both write access and read-only access for a feature, the Infranet Controller grants the most permissive access. For example, if you select the <b>Administrators can manage ALL roles</b> check box under Delegate User Roles, and then select the Users role on the Delegate As Read-Only Roles page, then the Infranet Controller allows the delegated administrator role full management privileges to the Users role.
<b>Admin Role &gt; General &gt; Users &gt; Realms &gt; Delegate User Realms</b>		
Administrators 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 from the Non—members list and add to the Members list.
Access	Specifies which user authentication realms pages that the delegated administrator can manage.	<ul style="list-style-type: none"> <li>■ Select <b>Write All</b> to specify that members of the administrator role can modify all user authentication realm pages.</li> <li>■ Select <b>Custom Settings</b> to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user authentication realm pages.</li> </ul>
<b>Admin Role &gt; General &gt; Users &gt; Realms &gt; Delegate As Read-Only Realms</b>		
Administrator can view (but not modify) ALL realms	Allows the administrator to view the user authentication realms, but not modify.	Select the user authentication realms that you want to allow the administrator to view.  <b>NOTE:</b> If you specify both write access and read-only access for an authentication realm page, the Infranet Controller grants the most permissive access. For example, if you select the <b>Administrators can manage ALL realms</b> check box under Delegate User Realms, and then select the Users role on the Delegate As Read-Only Realms page, then the Infranet Controller allows the delegated administrator role full management privileges to the Users realm.
<b>Admin Role &gt; General &gt; Delegated Administrator Settings &gt; Management of Admin roles</b>		
Manage ALL admin roles	Manages all admin roles.	Select to manage all the admin roles.

**Table 1: Administrator Role Configuration Details (continued)**

Option	Function	Your Action
Allow Add/Delete admin roles	Allows the security administrator the ability to create administrator roles, even if the security administrator is not part of the Administrators role.	Select to allow the security administrator to add and delete admin roles.
Access	Indicates the level of access that you want to allow the security administrator role to set for system administrators.	<ul style="list-style-type: none"> <li>■ Select <b>Deny All</b> to specify that members of the security administrator role cannot see or modify any settings in the category.</li> <li>■ Select <b>Read All</b> to specify that members of the security administrator role can view, but not modify, all settings in the category.</li> <li>■ Select <b>Write All</b> to specify that members of the security administrator role can modify all settings in the category.</li> <li>■ Select <b>Custom Settings</b> to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.</li> </ul>
<b>Admin Role &gt; General &gt; Delegated Administrator Settings &gt; Management of Admin realms</b>		
Manage ALL admin realms	Manages all admin realms.	Select to manage all the admin realms.
Allow Add/Delete admin realms	Allows the security administrator to create and delete administrator realms, even if the security administrator is not part of the administrators role.	Select to allow the security administrator to add and delete admin realms.
Access	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.	<ul style="list-style-type: none"> <li>■ Select <b>Deny All</b> to specify that members of the security administrator role cannot see or modify any settings in the category.</li> <li>■ Select <b>Read All</b> to specify that members of the security administrator role can view, but not modify, all settings in the category.</li> <li>■ Select <b>Write All</b> to specify that members of the security administrator role can modify all settings in the category.</li> <li>■ Select <b>Custom Settings</b> to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.</li> </ul> <p><b>NOTE:</b> All administrators that can manage admin roles and realms have at least read-only access to the admin role's Name and Description and to the realm's Name and Description, as displayed on the General page.</p>
<b>Admin Role &gt; General &gt; Delegated Resource Policies &gt; All tab</b>		

**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.	<ul style="list-style-type: none"> <li>■ Select <b>Deny All</b> to specify that members of the administrator role cannot see or modify any resource policies.</li> <li>■ Select <b>Read All</b> to specify that members of the administrator role can view, but not modify, all resource policies.</li> <li>■ Select <b>Write All</b> to specify that members of the administrator role can modify all resource policies.</li> <li>■ Select <b>Custom Settings</b> to allow you to pick and choose administrator privileges (Deny, Read, or Write) for each type of resource policy or for individual resource policies.</li> </ul>
<b>Admin Role &gt; General &gt; Delegated Resource Policies &gt; Custom Settings</b>		
Additional Access Policies	Sets custom access levels for an individual policy	Select the access level for the policy (Deny, Read, or Write).
Policies	Provides custom access level.	Select the resource policy for which you want to provide a custom access level, and click <b>Add</b> .
<b>Default Options for Delegated Admins &gt; Session Options tab</b>		
Idle Timeout (minutes)	Specifies the number of minutes an administrator session may remain idle before ending. The minimum is 5 minutes. The default idle session limit is ten minutes, which means that if an administrator's session is inactive for ten minutes, the Infranet Controller ends the session and logs the event in the system log (unless you enable session timeout warnings described below).	Enter the idle timeout duration in minutes.
Max. Session Length (minutes)	Specifies the number of minutes an active administrator session may remain open before ending. The minimum is 6 minutes. The default time limit for an administrator session is sixty minutes, after which the Infranet Controller ends the session and logs the event in the system log.	Enter the session length in minutes. The default is 300 seconds, and the minimum is six minutes.

**Table 1: Administrator Role Configuration Details (continued)**

Option	Function	Your Action
Roaming session	Roaming sessions allow users to work across source IP addresses. This is useful for mobile users with dynamically assigned IP addresses, as it allows them to sign in from their desk and continue working.	<ul style="list-style-type: none"> <li>■ Select <b>Enabled</b> to enable roaming user sessions for users mapped to this group. A roaming user session works across source IP addresses, which allows mobile administrators (laptop users) with dynamic IP addresses to sign in to the Infranet Controller from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This helps protect against an attack spoofing a user's session, provided the hacker was able to obtain a valid user's session cookie.</li> <li>■ Select <b>Limit to subnet</b> to limit the roaming session to the local subnet specified in the Netmask field. Administrators may sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet.</li> <li>■ Select <b>Disabled</b> to disable roaming sessions for administrators mapped to this role. Administrators who sign in from one IP address may not continue an active Infranet Controller session from another IP address; administrator sessions are tied to the initial source IP address.</li> </ul>
<b>Default Options for Delegated Admins &gt; UI Options tab</b>		
Logo image	Displays the logo in the Current appearance box only after you save your changes.	Click the Browse button and locate your custom image file.
Background color	Updates the current appearance of the box.	Type the hexadecimal number for the background color or click the Color Palette icon and pick the desired color.
Navigation Menus	Displays hierarchical navigation menus.	<ul style="list-style-type: none"> <li>■ Select <b>Auto-enabled</b> to determine whether the administrator is signed in from a supported platform and enables or disables the hierarchical menus accordingly.</li> <li>■ Select <b>Enabled</b> to enable hierarchical menus, regardless of your platform. If the administrator is signed in from an unsupported platform, they may not be able to use the hierarchical menus, even though they are enabled.</li> <li>■ Select <b>Disabled</b> to disable hierarchical menus for all members of the role.</li> </ul>

**Table 1: Administrator Role Configuration Details** (continued)

Option	Function	Your Action
Show copyright notice in footer	Specifies the copyright notice and label in the footer.	Select or clear the check box (optional).  <b>NOTE:</b> If you do not want user roles to see the copyright notice, you can also deselect the option in the Default Settings for user roles, in general. That way, all subsequent roles you create do not allow the notice to appear on the end-user UI.

- Related Topics**
- Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure)
  - Configuring Infranet Controller User Roles (NSM Procedure)
  - Configuring Access Options on an Infranet Controller User Role (NSM Procedure)
  - Configuring OAC Settings for a User Role (NSM Procedure)

---

Published: 2009-08-20