

Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure)

You can delegate management tasks to various delegated administrator roles.

To delegate management tasks to administrator roles:

1. In the 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 under **Admin Role** as specified in Table 1.
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 1: Administrator Role Configuration for Delegation

Option	Function	Your Action
Users > Roles > Delegate User Roles		
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 Add to move it to the Members list.
Access	Specifies which user role pages the delegated administrator can manage.	<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.
Users > Role > Delegate As Read-Only Role		
Administrator can view (but not modify) ALL roles	Allows the administrator to view the user roles, but not manage.	<p>Select the user roles that you want to allow the administrator to view.</p> <p>NOTE: 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 Administrators can manage ALL roles 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.</p>

Table 1: Administrator Role Configuration for Delegation (continued)

Option	Function	Your Action
Users > Realms > Delegate User Realms		
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 in the Non-members list and click Add to move it to the Members list.
Access	Specifies which user authentication realms pages that the delegated administrator can manage.	<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.
Users > 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 Infranet Controller grants the most permissive access. For example, if you select the Administrators can manage ALL realms 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.</p>
Delegated System Settings tab		
System Tasks	Indicates the level of access that you want to allow for system tasks.	<ul style="list-style-type: none"> ■ Select Deny All to specify that members of the administrator role cannot view or modify any settings.
Log/Monitoring	Indicates the level of access that you want to allow for log/monitoring.	<ul style="list-style-type: none"> ■ Select Read All to specify that members of the administrator role can view, but not modify settings.
Authentication	Indicates the level of access that you want to allow for authentication.	<ul style="list-style-type: none"> ■ Select Write All to specify that members of the administrator role can modify all settings.
Maintenance Tasks	Indicates the level of access that you want to allow for maintenance tasks.	<ul style="list-style-type: none"> ■ Select Custom Settings to allow you to pick and choose privileges (Deny, Read, or Write) for System, Archiving and Troubleshooting pages.
Delegated Administrator Settings > Management of Admin roles		
Manage ALL admin roles	Manages all admin roles.	Select to manage all the admin roles.

Table 1: Administrator Role Configuration for Delegation (continued)

Option	Function	Your Action
Allow Add/Delete admin roles	Allows the security administrator 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"> ■ Select Deny All to specify that members of the security administrator role cannot see or modify any settings in the category. ■ Select Read All to specify that members of the security administrator role can view, but not modify, all settings in the category. ■ Select Write All to specify that members of the security administrator role can modify all settings in the category. ■ Select Custom Settings to allow 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 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 (General, Authentication Policy, and Role Mapping.)	<ul style="list-style-type: none"> ■ Select Deny All to specify that members of the security administrator role cannot see or modify any settings in the category. ■ Select Read All to specify that members of the security administrator role can view, but not modify, all settings in the category. ■ Select Write All to specify that members of the security administrator role can modify all settings in the category. ■ Select Custom Settings to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category. <p>NOTE: 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 tab.</p>

Table 1: Administrator Role Configuration for Delegation (continued)

Option	Function	Your Action
Delegated Resource Policies > All tab		
Access	Indicates the level of access that you want to allow the administrator role for each Resource Policies sub-menu	<ul style="list-style-type: none"> ■ Select Deny All to specify that members of the administrator role cannot see or modify any resource policies. ■ Select Read All to specify that members of the administrator role can view, but not modify, all resource policies. ■ Select Write All to specify that members of the administrator role can modify all resource policies. ■ Select Custom Settings to allow you to pick and choose administrator privileges (Deny, Read, or Write) for each type of resource policy or for individual resource policies.
Delegated Resource Policies > All (Custom Settings for Infranet Enforcer, Network Access, and Host Enforcer)		
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 Add .

- Related Topics**
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure)
 - Configuring Infranet Controller User Roles (NSM Procedure)
 - Configuring OAC Settings for a User Role (NSM Procedure)
 - Configuring Access Options on an Infranet Controller User Role (NSM Procedure)

Published: 2009-08-20