

## Configuring Infranet Controller User Roles (NSM Procedure)

A user role defines user session parameters and personalization settings. You can customize a user role by specifying access restrictions, enabling Host Enforcer (Windows) or agentless or Java agent access, and configuring session settings. You can create and configure user roles through the User Roles page from the Infranet Controller device configuration tree.

To configure a user 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 the user roles.
3. Click the **Configuration** tab. In the configuration tree, select **Users > User Roles**. The corresponding workspace appears.
4. Click the **New** button, the New dialog box appears.
5. Add or modify settings on the General tab as specified in Table 1.
6. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 1: User Role Configuration Details**

| Option                                       | Function  | Your Action   |
|--|---|---|
| <b>General &gt; Overview tab</b>             |   |   |
| Name   | Specifies a unique name for the user role.  | Enter a name.   |
| Description                                  | Describes the user role.  | Enter a brief description for the user 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 customized settings for the Infranet Controller welcome page for Odyssey Access Client users mapped to this role. | Select <b>General &gt; UI Options</b> to apply the settings to the role.                        |
| Odyssey Settings for IC Access               | Specifies the Odyssey Access Client settings for Infranet Controller access.  | Select this option to apply the Odyssey Access Client initial configuration settings.           |
| Odyssey Settings for Preconfigured Installer | Specifies the Odyssey Access Client settings for the preconfigured installer.   | Select this option to apply the Odyssey Access Client settings for the preconfigured installer. |

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

| Option                                  | Function   | Your Action   |
|---|--|---|
| <b>General &gt; Restrictions tab</b>    |  |   |
| Source IP Restrictions                  | Specifies source IP restrictions.  | See "Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)."  |
| Browser Restrictions                    | Specifies browser restrictions.  | See "Configuring Infranet Controller Browser Access Restrictions (NSM Procedure)."  |
| Certificate Restrictions                | Specifies certificate restrictions.  | See "Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure)."  |
| Host Checker Restrictions               | Specifies Host Checker restrictions.   | See "Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure)."   |
| <b>General &gt; Session Options tab</b> |  |   |
| Max. Session Length (minutes)           | Specifies the number of minutes an active nonadministrative user session may remain open before ending. During an end-user session, prior to the expiration of the maximum session length, the Infranet Controller prompts the user to reenter authentication credentials, which avoids the problem of terminating the user session without warning. | Enter the session length in minutes. The default is five minutes, and the minimum is six minutes.   |
| Heartbeat Interval (seconds)            | Specifies the frequency at which the endpoint should send out a heartbeat to the Infranet Controller to keep the session alive. For agentless access, the browser refreshes the page with every heartbeat.   | Enter the heartbeat interval in seconds.<br><br>Users should not navigate away from the browser, as this interrupts the heartbeat and ends the session. The Odyssey Access Client and the Java agent respectively provide the heartbeat. You should ensure that the heartbeat interval of the agent is greater than the Host Checker interval, otherwise performance could be affected. |
| Heartbeat Timeout (seconds)             | Specifies the amount of time that the Infranet Controller should "wait" before terminating a session when the endpoint does not send a heartbeat response.   | Enter the heartbeat timeout in seconds.   |

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

| Option                               | Function   | Your Action  |
|--------------------------------------|--|--|
| Roaming session                      | <ul style="list-style-type: none"> <li>■ <b>Enabled</b>—Enables roaming user sessions for users mapped to this role. A roaming user session works across source IP addresses, which allows mobile users (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>■ <b>Limit to subnet</b>—Limits the roaming session to the local subnet specified in the Netmask field. Users 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>■ <b>Disabled</b>—Disables roaming user sessions for users mapped to this role. Users who sign in from one IP address may not continue an active Infranet Controller session from another IP address; user sessions are tied to the initial source IP address.</li> </ul> | Select this option to enable, limit, or disable the roaming session.   |
| Roaming netmask                      | Displays the netmask for the local subnet.   | Select this option to view the netmask for the local subnet.   |
| Enable Session Extension             | Allows users with a Layer 2 or Layer 3 connection to continue a session beyond the maximum session length.   | Select this option to allow users with Odyssey Access Client and agentless access to reauthenticate and extend their current session without interruption. |
| <b>General &gt; UI Options tab</b>   |  |  |
| <b>Headers &gt; Logo image</b>       | Displays the logo in the Infranet Controller welcome page.   | Browse to your custom image file.  |
| <b>Headers &gt; Background color</b> | Displays the background color for the header area of the Infranet Controller welcome page.   | Type the hexadecimal number for the background color, or click the Color Palette icon and pick the desired color.  |

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

| Option  | Function  | Your Action   |
|---|---|---|
| <b>Greeting &gt; Show notification message</b>  | Enables the notification text box.  | Select the <b>Show notification message</b> check box (optional).   |
| <b>Greeting &gt; Notification Message</b>   | Displays the notification message at the top of the Infranet Controller welcome page. | <p>Enter the message that you want to display.</p> <p>You may format text and add links using the following HTML tags: <code>&lt;i &gt;</code>, <code>&lt;b &gt;</code>, <code>&lt;br &gt;</code>, <code>&lt;font &gt;</code>, and <code>&lt;a href &gt;</code>. However, the Infranet Controller does not rewrite links on the sign-in page (because the user has not yet authenticated), so you should only point to external sites. Links to sites behind a firewall will fail. You may also use Infranet Controller system variables and attributes in this field.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>■ The length of the personalized greeting cannot exceed 12K or 12288 characters.</li> <li>■ If you use unsupported HTML tags in your custom message, the Infranet Controller may display the end user's Infranet Controller home page incorrectly.</li> </ul> |
| <b>Other &gt; Show copyright notice and 'Secured by Juniper Networks' label in footer</b> | Displays the copyright notice and label in the footer.                                | <p>Select the <b>Show copyright notice and 'Secured by Juniper Networks' label in footers</b> check box (optional).</p> <p>This setting applies only to those users whose license permits disabling the copyright notice. For more information about this feature, call Juniper Networks Support.</p>   |

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