

## Configuring Infranet Controller Browser Access Restrictions (NSM Procedure)

Browser restrictions control from which Web browsers users can access an Infranet Controller sign-in page or be mapped to a role. If a user tries to sign into the Infranet Controller using an unsupported browser, the sign-in attempt fails and a message displays stating that an unsupported browser is being used. This feature also ensures that users sign into the Infranet Controller from browsers that are compatible with corporate applications or are approved by corporate security policies.

To configure Infranet Controller browser access restrictions:

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 browser access restrictions.
3. Click the **Configuration** tab. In the configuration tree, select the level at which you want to implement browser access restrictions:
  - Realm level—Select:
    - **Administrators > Admin Realms > Select Realm > Authentication Policies > Browser** to configure browser access restrictions for admin realms.
    - **Users > User Realms > Select Realm > Authentication Policies > Browser** to configure browser access restrictions for user realms.
  - Role level—Select:
    - **Administrators > Admin Roles > Select Role > General > Restrictions > Browser Restrictions** to configure browser access restrictions for admin roles.
    - **Users > User Roles > Select Role > General > Restrictions > Browser Restrictions** to configure browser access restrictions for user roles.
4. 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: Browser Access Restrictions Configuring Details**

Option	Function	Your Action
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>

**Table 1: Browser Access Restrictions Configuring Details** (continued)

Option	Function	Your Action
User-Agent pattern	Specifies the user agent string pattern.	Enter a string in the format  * < browser_string > *  where start (*) is an optional character used to match any character and < browser_string > is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser.  <b>NOTE:</b> You cannot include escape characters (\) in browser restrictions.
Action	Specifies whether to allow or deny browser 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>

- Related Topics**
- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)
  - Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure)
  - Configuring Infranet Controller Password Access Restrictions (NSM Procedure)
  - Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure)
  - Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure)
  - Configuring Infranet Controller User Roles (NSM Procedure)
  - Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure)