

Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)

Source IP access restrictions control from which IP addresses users can access an Infranet Controller sign-in page, be mapped to a role, or access a resource.

To configure Infranet Controller source IP access restrictions:

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 source IP access restrictions.
3. Click the **Configuration** tab. In the Configuration tree, select:
 - **Administrators > Admin Roles > Select Role > General > Restrictions > Source IP Restrictions** to configure source IP access restrictions for admin roles.
 - **Administrators > Admin Realms > Select Realm > Authentication Policies > Source IP** to configure source IP access restrictions for admin realms.
 - **Users > User Roles > Select Role > General > Restrictions > Source IP Restrictions** to configure source IP access restrictions for user roles.
 - **Users > User Realms > Authentication Policies > Source IP** to configure source IP access restrictions for user realms.
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: Source IP Access Restrictions Configuration Details

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"> ■ Select Users from any IP address to enable users to sign into the Infranet Controller from any IP address. ■ Select Users from IP addresses which pass the specified matching policies to allow access only to the listed IP addresses.
Source IP Address	Specifies the source IP address.	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"> ■ Select Allow to allow the user to use the IP address. ■ Select Deny to prevent users from using the IP address.

Table 1: Source IP Access Restrictions Configuration Details (continued)

Option	Function	Your Action
Enable Administrators to sign in on the External Port	Specifies whether or not administrators can sign in from the external port	Select this option to enable administrators to sign in on the external port.. NOTE: This setting can be configured only for admin realms.
Enable Administrators to sign in on the Internal Port	Specifies whether or not administrators can sign in from the internal port.	Select this option. NOTE: This setting can be configured only for admin realms.

Related Topics

- Configuring Infranet Controller Browser 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)