

Configuring Infranet Controller Authentication Policies (NSM Procedure)

An authentication policy is a set of rules that controls one aspect of access management—whether or not to present a realm’s sign-in page to a user. An authentication policy is part of an authentication realm’s configuration, specifying rules for the Infranet Controller to consider before presenting a sign-in page to a user. If a user meets the requirements specified by the realm’s authentication policy, then the Infranet Controller presents the corresponding sign-in page to the user and forwards the user’s credentials to the appropriate authentication server. If this server successfully authenticates the user, then the Infranet Controller moves on to the role evaluation process.

To configure an authentication realm policy:

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 an authentication realm policy.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators > Admin Realms** or **Users > User Realms**.
4. Add or modify authentication realm policy settings in the Authentication Policies tab for one or more of the access management options.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- Related Topics**
- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)
 - Configuring Infranet Controller Browser Access Restrictions (NSM Procedure)
 - Configuring Infranet Controller Certificate 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)

