

Configuring Infranet Controller RADIUS Request Attribute Restrictions for User Realms (NSM Procedure)

You can create RADIUS request attribute policies to require authentication requests to contain specific RADIUS attribute values. If an endpoint attempts to access a realm with a RADIUS request attribute policy, the endpoint must meet the conditions specified in the policy.

To add a RADIUS request attribute policy to a realm:

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 RADIUS request attribute restrictions for user realms.
3. From the Configuration tab, select **Users > User Realms > Select Realm > Authentication Policies > RADIUS Request Attributes Policies** to configure RADIUS request attribute restrictions for user realms.
4. Select the RADIUS request attribute policies, which the endpoint must meet, from the Non-members area and click **Add** to move it to the Members area.
5. Select **Allow access to realm if any ONE of the selected policies are passed**.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- Related Topics**
- [Configuring RADIUS Request Attributes Policies \(NSM Procedure\)](#)
 - [Configuring Infranet Controller Source IP Access Restrictions \(NSM Procedure\)](#)
 - [Configuring Infranet Controller Browser 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 \(NSM Procedure\)](#)

Published: 2009-08-20