

Configuring an Infranet Controller to Connect to a JUNOS Enforcer (NSM Procedure)

You can use a JUNOS Enforcer with the UAC solution. A JUNOS Enforcer is a J Series Services Router or an SRX Series Services Gateway configured as a Layer 3 enforcement point. See the Unified Access Control Supported Platforms document for compatibility. The JUNOS Enforcer connects with the Infranet Enforcer over an SSL connection. To initiate the connection between the two appliances, you must specify the password and serial number of the JUNOS Enforcer.

To configure the Infranet Controller to accept a connection from the JUNOS Enforcer:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller that you want to configure.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > Connection**.
4. Click **New (+)**. The New Infranet Enforcer dialog box appears. By default, the ScreenOS Enforcer options are displayed.
5. Select the **JUNOS** option button. The JUNOS Enforcer page appears.
6. Enter the name and password of the Infranet Enforcer.
7. Enter the serial number(s) of the JUNOS Enforcer. You can view the serial number on the JUNOS Enforcer using the command:

`show chassis hardware`
8. To configure IDP, select **Use IDP Module**. For more information on configuring ISG-IDP on a enforcer, refer to [\[Unresolved xref\]](#).



NOTE: For the Infranet Controller to interoperate with IDP, the ic-xxxx-ADD-tctrl coordinated threat control license is required.

9. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- Related Topics**
- [Configuring an Infranet Controller to Connect to a ScreenOS Enforcer \(NSM Procedure\)](#)
 - [Configuring Infranet Controller Source IP Access Restrictions \(NSM Procedure\)](#)
 - [Configuring Infranet Controller Host Enforcer Policies \(NSM Procedure\)](#)

Published: 2009-08-20