

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

The ScreenOS Enforcer connects to the Infranet Controller over an SSH connection that uses the NetScreen Address Change Notification (NACN) protocol.

The Infranet Controller uses the NACN password and serial number for a connection from the ScreenOS Enforcer. When the ScreenOS Enforcer first turns on, it sends an NACN message containing the NACN password and serial number to the Infranet Controller. The Infranet Controller uses the serial number to determine which ScreenOS Enforcer is attempting to connect, and then the Infranet Controller uses the NACN password to authenticate the ScreenOS Enforcer. The Infranet Controller then begins communicating with the ScreenOS Enforcer using SSH.

To configure the Infranet Controller to accept a connection from the ScreenOS 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.
5. Select the **ScreenOS** option button from the Platform area. The ScreenOS Enforcer page appears.
6. Enter a name for the ScreenOS Enforcer.
7. Enter an NACN password for this Infranet Enforcer in the NACN password box. You must enter this same NACN password when configuring the ScreenOS Enforcer.
8. Enter the administrator name and administrator password for signing into the ScreenOS Enforcer.
9. Enter the serial number(s) of the ScreenOS Enforcer. You can view the serial number on the home page of the Infranet Enforcer WebUI, or by entering the following Juniper Networks ScreenOS CLI command:

```
get system
```
10. To configure ISG-IDP, select **Use IDP Module**. For more information on configuring ISG-IDP on an 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.

11. Select **No 802.1X** from the Location Group list if you are not using an Infranet Enforcer as an 802.1X RADIUS client of the Infranet Controller.
12. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

- Related Topics**
- Configuring an Infranet Enforcer as a RADIUS Client of the Infranet Controller (NSM Procedure)
 - Configuring an Infranet Controller to Connect to a JUNOS Enforcer (NSM Procedure)
 - Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)
 - Configuring Infranet Controller Host Enforcer Policies (NSM Procedure)

Published: 2009-08-20