

## Importing a Secure Access Device

---

You can add a Secure Access device to your existing network by using NSM and importing its configurations. Using the Add Device Wizard, you can configure a connection between the management system and the physical device, and then import all device parameters, policies, objects, VPNs, and so on.

Import a Secure Access device by following these procedures:

1. Installing and Configuring a Secure Access Device on page 1
2. Adding a Secure Access Device Through NSM on page 2
3. Configuring and Activating the NSM agent on the Secure Access Device on page 3
4. Confirming Connectivity and Importing the Secure Access Device Configuration on page 3

### Installing and Configuring a Secure Access Device

Before you add the Secure Access device to NSM, you must install and configure the Secure Access device to have logon credentials for an NSM administrator.

To install and configure a Secure Access device:

1. Select **System > Network > Overview** in the device's admin console and ensure that basic connection information such as the following are configured on the Secure Access device:
  - Network interface settings
  - DNS settings
  - Password
2. Select **Authentication > Auth Servers** and enter the username and password of the NSM administrator in the applicable authentication server.



**NOTE:** Only password-based authentication servers can be used. One-time password authentication is not supported.

---

3. Select **Administrators > Admin Roles** and create an NSM agent role.
4. Select **Administrators > Admin Realms** and create an NSM agent administrator realm for the DMI agent on the Secure Access device and use role mapping to associate the NSM agent role and realm. Do not apply any role or realm restrictions for the NSM agent role or realm.

For complete details on installing and configuring Secure Access devices, see the *Juniper Networks Secure Access Administration Guide*.

## Adding a Secure Access Device Through NSM

To add the Secure Access device through the NSM UI:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and Select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Device**. The New-Device dialog box appears.
4. Select **Device is Not Reachable** and click **Next**.
5. Enter the device name, and select the required color, OS name (SA), and platform and managed OS version from the drop-down lists.
6. From the Choose Device Server Connection Parameter area, select:
  - **Use Default Device Server IP Address and Port** — Connects the device to the NSM Device Server IP address and port.
  - **Use Device Server Through MIP** — Connects the NSM device server through a mapped IP address and port.
7. Click **Next**, and a unique external ID gets generated automatically. This ID represents the device within the management system.
8. Enter an admin username for the device admin.
9. Set the Admin User Password and the First Connection One-Time Password:
  - Select **Set Password** and enter a new password.
  - Confirm your new password and click **OK**.



### NOTE:

- Make a note of the unique external ID. The device administrator will need it to configure connectivity with NSM. The wizard automatically enters this value for the device. This ID number represents the device within the management system.
- Specify the administrator username and password for the SSH connection. This name and password must match the name and password already configured on the device.
- Specify the First Connection One Time Password (OTP) that authenticates the device. Make a note of this password. The device administrator will need it to configure the connectivity with NSM.

- 
10. Click **Finish** to add the device to the NSM UI. The newly added Secure Access device appears in the Devices workspace.

## **Configuring and Activating the NSM agent on the Secure Access Device**

You must configure and activate the NSM agent on the Secure Access device. It establishes the SSH communications with the NSM application and controls the Secure Access device from the NSM application.

To configure and activate the NSM agent:

1. Select **System > Configuration > DMI Agent** to add the NSM management application.
2. Under DMI settings for outbound connections, enter the device server's IP address in the Primary Server box.
3. Enter **7804** in the Primary Port box.
4. Fill in the Backup Server and Backup Port boxes, if a device server is configured for high availability.
5. Enter the unique external ID provided by the NSM administrator in the Device ID box.
6. Enter the first connection one-time password provided by the NSM administrator in the HMAC box.
7. Click **Enable** to activate the NSM agent.
8. Click **Save Changes**, and the device attempts to establish a session with the NSM application.

The device software initiates the TCP connection to NSM and identifies itself using the specified device ID and HMAC. Both sides then engage in SSH Transport Layer interactions to set up an encrypted tunnel. The Inbound and Outbound DMI connections enabled facilitates the DMI connection. The DMI uses the specified admin realm to login to the device. The NSM application authenticates itself to the Secure Access device based on username and password.

## **Confirming Connectivity and Importing the Secure Access Device Configuration**

To confirm connectivity:

1. From the Devices workspace, select the **Device List** tab.
2. Check the newly added device in the Connection Status column. The connection status must change from Never Connected to Up.

If the connection status appears as Device Platform Mismatch or Device Firmware Mismatch, delete the device from the application and add it back using the correct device platform and managed OS, respectively.

To import the device configuration:

1. From the Devices workspace, select the **Device List** tab.
2. Right-click the newly added Secure Access device and select **Import Device**. The Save Changes dialog box appears.

3. Click **Yes** to save policy or VPN changes. The Device Import Option dialog box appears.
4. Select **Run Summarize Delta Config**, click **OK** and **Yes**. The Job Information dialog box displays the progress of the delta config summary. You can also monitor the progress in the Job Manager.

The next step is to verify the imported configuration using either the Device Monitor or the Device Manager in NSM. See “Verifying Imported Device Configurations” for details.

- Related Topics**
- Importing Multiple Secure Access Devices
  - Verifying Imported Device Configurations
  - Creating and Applying a Secure Access Device Template

---

Published: 2009-08-20