

## **NSM and Intrusion Detection and Prevention Device Management Overview**

---

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer Intrusion Detection Prevention (IDP) device configurations.

With NSM, you can manage most of the parameters that you can configure through the IDP admin console. The configuration screens rendered through NSM are similar to the screens in the IDP admin console. NSM incorporates a broad configuration management framework that allows co-management using other methods.

After you have completed installation, follow the below steps to get started with managing IDP device with NSM:

1. Add IDP device to NSM. When you add the IDP device to NSM in first instance, NSM pushes the policy named Recommended to the device.
2. Update the IDP detector engine and attack object database.
3. Update software version (if necessary).
4. Run the profiler.
5. Examine the logs.
6. Create address objects for IDP rulebase rules.
7. Optionally, configure additional rulebases.
8. If adding these device changes your plan to distribute administrative responsibility, create NSM users with the access privileges.

- Related Topics**
- [Intrusion Detection and Prevention Services and Device Configurations Supported in NSM](#)
  - [Adding Intrusion Detection and Prevention Devices in NSM Overview](#)

