# Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Juniper Networks NetScreen Firewall

Release 6 (2.1.1.0.0)

**E11850-01**

December 2007

This document provides a brief description about the Oracle System Monitoring Plug-in for Juniper Networks NetScreen Firewall, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

## Description

The System Monitoring Plug-in for Juniper Networks NetScreen Firewall extends Oracle Enterprise Manager Grid Control to add support for managing NetScreen Firewalls. By deploying the plug-in in your Grid Control environment, you gain the following management features:

- Monitor Juniper Networks NetScreen Firewall devices.
- Gather configuration data and track configuration changes for Juniper Networks NetScreen Firewall instances.
- Raise alerts and violations based on thresholds set on monitoring and configuration data.
- Provide rich out-of-box reports for the user interface based on the gathered data.
- Support monitoring by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as NetScreen Firewall.
- Juniper NetScreen Plug-in supports monitoring of status of the devices configured in NSRP Clusters. It generates alerts when the status of the firewall changes from Master to other states (such as Primary Backup, Ineligible, and Inoperable). Also, provides 'clear message' when the firewall is back to Master status.

> **Note:** NetScreen Redundancy Protocol (NSRP) is a proprietary protocol that is supported on select NetScreen devices to provide high availability (HA) services. An NSRP cluster consists of a group of NetScreen devices that enforce the same overall security policy and share the same configuration settings. Refer to NetScreen documentation for details.

## Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10*g* Release 2 or higher Management Service and Agent
- Juniper Networks NetScreen Firewalls that have ScreenOS version 5.0.0 or higher, and that are backward-compatible with ScreenOS version 5.0.0. The following versions of NetScreen Firewall are supported:
  - NetScreen-5 Series
  - NetScreen-25/50
  - NetScreen-204/208
  - NetScreen-500
  - NetScreen-5200/5400
  - ISG Series

## Prerequisites

The following prerequisites must be installed before you can deploy the plug-in:

- Oracle Enterprise Manager Grid Control 10*g* Release 2 or higher system and Agent
- NetScreen Firewall instance
- The Agent's IP address must be added to any configured SNMP community on the NetScreen Firewall. See "Adding the Agent's IP Address" for procedures
- For Linux, the firewall SNMP daemon must be running on the NetScreen Firewall device
- For Windows, the standard Windows SNMP agent must be installed, and the SNMP Service must be running

## Deploying the Plug-in

After you ensure that the prerequisites are met, follow these steps to deploy the plug-in:

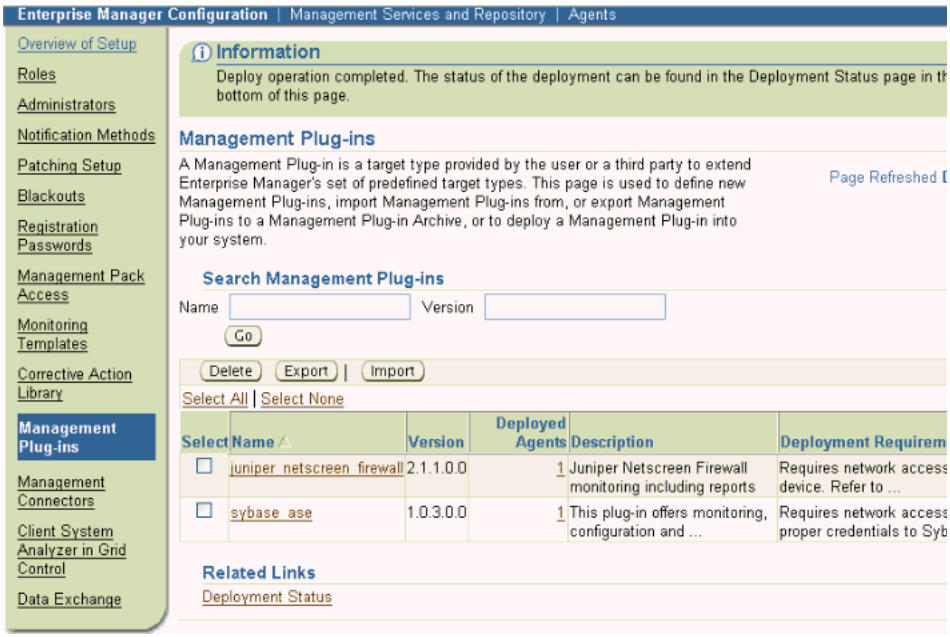
1. Download the Juniper Networks NetScreen Firewall Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log in to Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.
5. Click **Browse** and select the plug-in archive.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.
8. Verify that you have set preferred credentials on all Agents where you want to deploy the plug-in.

9. In the Management Plug-ins page, click the icon in the **Deploy** column for the NetScreen Firewall plug-in. The Deploy Management Plug-in wizard appears.
10. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.
11. Click **Next**, then click **Finish**.

    If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type and host target type on which the Agent resides.

    If there are no errors, you can see the following screen:

***Figure 1 Successful Deployment***




## Adding Instances for Monitoring

After successfully deploying the plug-in, follow these steps to add the plug-in target to Grid Control for central monitoring and management:

1. From the Agent Home page where the Juniper Networks NetScreen Firewall Plug-in was deployed, select the **NetScreen Firewall** target type from the **Add** drop-down list, then click **Go**. The Add Juniper NetScreen Firewall page appears.
2. Provide the following information for the properties:
   - **Name —** A name for the plug-in, such as My Juniper 1.
   - **Firewall Hostname or IP Address —** The name or IP address of the NetScreen Firewall to be monitored.

- **Host SNMP Daemon Port —** The port number on the NetScreen Firewall where the native OS SNMP domain is running. The default is 161.

  You can determine the port number by using the command `get snmp settings` on the NetScreen Firewall command line interface, or by doing the following from the Web interface of the firewall:

  – Click on the **Configuration** link.

  – Click on the **Report Settings** link.

  – Click on the **SNMP** link.

  The value specified on the listen port on the Web UI is the SNMP daemon port.

- **SNMP Community —** The SNMP community name to which the Agent's IP address is added. The default is Public.

  You can determine the community name by using the command `get snmp settings` on the NetScreen Firewall command line interface, or by doing the following from the Web interface of the firewall:

  – Click on the **Configuration** link.

  – Click on the **Report Settings** link.

  – Click on the **SNMP** link.

  – Select the community to which you have added the Enterprise Manager Agent's IP address.

- **SNMP Timeout —** The timeout value at which the SNMP call should be terminated. The default value is 5 seconds.

- **Telnet Enabled (y/n) —** If telnet is enabled on the NetScreen Firewall device, specify the default of **y**. Otherwise, leave this field blank.

3. Click **Test Connection** to make sure the parameters you entered are correct.

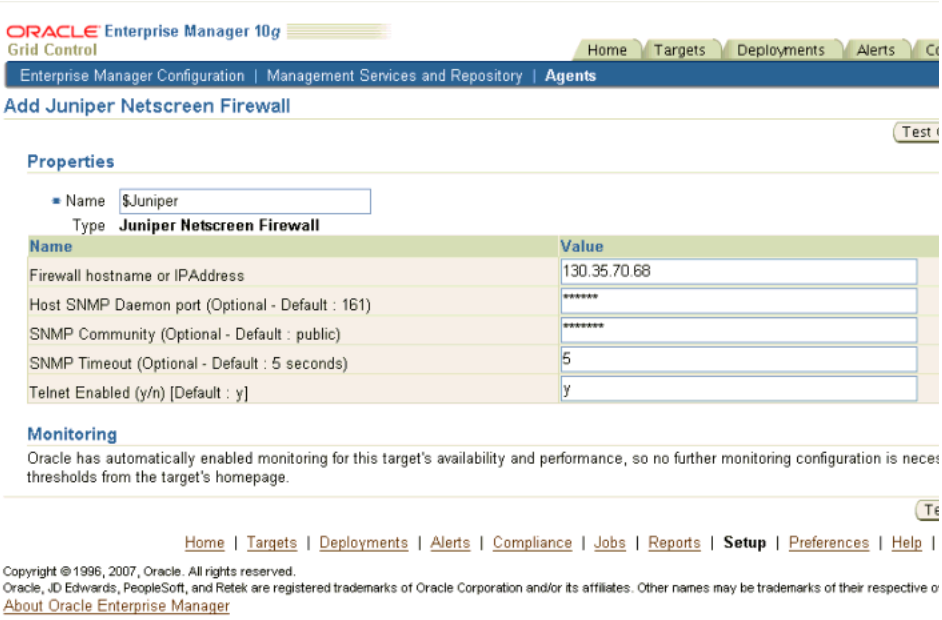
4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**.

---

**Note:** After you deploy and set up the plug-in to monitor one or more targets in the environment, you can customize the plug-in monitoring settings to alter the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is a part of.

---

*Figure 2 Add Juniper Netscreen Firewall Page*

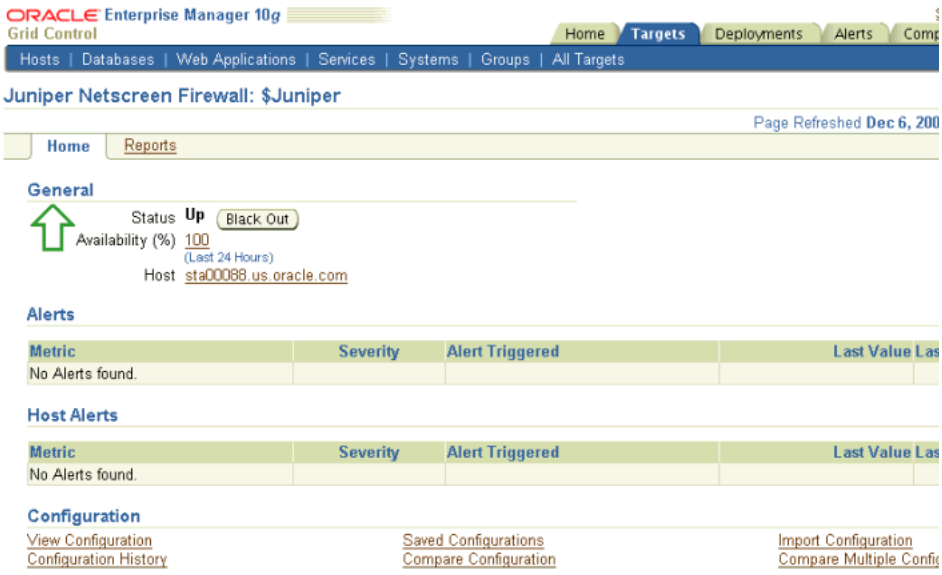



## Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the Juniper NetScreen Firewall target link from the Agent home page Monitored Targets table. The Juniper NetScreen Firewall home page appears.

*Figure 3 Juniper Netscreen Firewall Home Page*



2. Verify that no metric collection errors are reported in the Metrics table.
3. Ensure that reports can be seen and no errors are reported by clicking the **Reports** subtab.
4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not immediately appear, click **Refresh** in the View Configuration page.

## Adding the Agent's IP Address

To add the Agent's IP address to an existing SNMP community on the Juniper Networks NetScreen Firewall, do the following:

1. Go to the Web interface of the target NetScreen Firewall.
2. Click the **Configuration** link.
3. Click the **Report Settings** link.
4. Click the **SNMP** link.
5. Click **Edit** for the community to which you want to add the Agent.
6. Enter the following information for the properties, then click **Go**:
   - **Permissions —** Select from Write, Trap, and Including Traffic Alarms.
     - **Write —** Select to assign read-write privileges for MIB II data to the SNMP community. Otherwise, clear to assign read-only privileges.
     - **Trap —** Select to send notifications or 'traps' to the community. The NetScreen device sends Cold Start/Link Up/Link Down traps to all hosts in communities that you set to receive traps.
     - **Including Traffic Alarms —** Select to send traffic alarms to the SNMP community.
   - **Version —** Select V1.
   - **Host IP Address/Netmask —** Enter the IP addresses and netmask of the Agent.
   - **Source Interface —** Indicate the interface from which SNMP messages originate.

To alternatively add a new SNMP community, do the following:

1. Go to the Web interface of the target NetScreen Firewall.
2. Click the **Configuration** link.
3. Click the **Report Settings** link.
4. Click the **SNMP** link.
5. Click the **New Community** link.

   The New Community link is not found if three SNMP communities are already configured on the firewall. The NetScreen device administrator can create up to three SNMP communities with up to eight hosts in each community. In this case, edit any of the existing SNMP communities as explained at the beginning of this section.
6. Enter the following information for the properties, then click **Go**:

- **Community Name —** Enter the name of the group, or 'community,' of administrators permitted to view the data gathered by the SNMP agent and receive SNMP notification of system events.
- **Permissions —**
  - **Write —** Select to assign read-write privileges for MIB II data to the SNMP community. Otherwise, clear to assign read-only privileges.
  - **Trap —** Select to send notifications or 'traps' to the community. The NetScreen device sends Cold Start/Link Up/Link Down traps to all hosts in communities that you set to receive traps.
  - **Including Traffic Alarms —** Select to send traffic alarms to the SNMP community.
- **Version —** Select V1.
- **Hosts IP Address/Netmask —** Enter the IP addresses and netmasks of the hosts (workstations or subnets) that you want to define as members of the community.
- **Trap Version —** Select V1.
- **Source Interface —** Indicate the interface from which SNMP messages originate.

## Undeploying the Plug-in

Follow these steps to undeploy the plug-in from an Agent:

1. Log in to Enterprise Manager Grid Control as a Super Administrator.
2. Select the **Targets** tab, then the **All Targets** subtab. The All Targets page appears.
3. Select the Juniper NetScreen Firewall Plug-in target and click **Remove**. You must do this step for all targets of the plug-in.
4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
5. Click the **Setup** link in the upper right corner of the All Targets page, then click the Management Plug-ins link on the left side of the Setup page. The Management Plug-ins page appears.
6. Click the icon in the **Undeploy** column for the NetScreen Firewall plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the NetScreen Firewall Plug-in and click **OK**.

   You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.
8. Select the Juniper NetScreen Firewall plug-in on the Management Plug-ins page and click **Delete**.

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our

documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

### Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

### Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

### TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

---

System Monitoring Plug-in Installation Guide for Juniper Networks NetScreen Firewall, Release 6 (2.1.1.0.0)
E11850-01