# Device Administration Features

Modified: 2019-02-13

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net



*Device Administration Features*


The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

# List of Figures



# List of Tables

# About the Documentation



## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

## Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

*Table 1: Notice Icons*

| Icon | Meaning | Description |
|---|---|---|
|  | Informational note | Indicates important features or instructions. |
|  | Caution | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning | Alerts you to the risk of personal injury or death. |
|  | Laser warning | Alerts you to the risk of personal injury from a laser. |
|  | Tip | Indicates helpful information. |
|  | Best practice | Alerts you to a recommended use or implementation. |

Table 2 on page x defines the text and syntax conventions used in this guide.

*Table 2: Text and Syntax Conventions*

| Convention | Description | Examples |
|---|---|---|
| **Bold text like this** | Represents text that you type. | To enter configuration mode, type the **configure** command:<br><br>user@host> **configure** |
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host>` **show chassis alarms**<br><br>`No alarms currently active` |
| *Italic text like this* | • Introduces or emphasizes important new terms.<br>• Identifies guide names.<br>• Identifies RFC and Internet draft titles. | • A policy *term* is a named structure that defines match conditions and actions.<br>• *Junos OS CLI User Guide*<br>• RFC 1997, *BGP Communities Attribute* |
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br><br>[edit]<br>root@# **set system domain-name** *domain-name* |

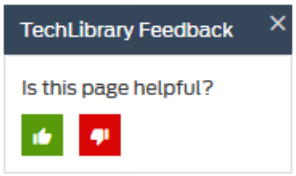
*Table 2: Text and Syntax Conventions (continued)*

| Convention | Description | Examples |
|---|---|---|
| **Text like this** | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | • To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level.<br>• The console port is labeled **CONSOLE**. |
| < > (angle brackets) | Encloses optional keywords or variables. | **stub <default-metric *metric*>;** |
| \| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | **broadcast \| multicast**<br><br>**(*string1* \| *string2* \| *string3*)** |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | **rsvp { # Required for dynamic MPLS only** |
| [ ] (square brackets) | Encloses a variable for which you can substitute one or more values. | **community name members [ *community-ids* ]** |
| Indention and braces ( { } ) | Identifies a level in the configuration hierarchy. | [edit]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| GUI Conventions | | |
| **Bold text like this** | Represents graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select **All Interfaces**.<br>• To cancel the configuration, click **Cancel**. |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select **Protocols>Ospf**. |

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:




  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/

- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

PART 1

# Overview

CHAPTER 1

# Device Administration Overview



## Device Administration Options for ScreenOS Devices Overview

Use the Device Administration screens to configure administrative options for the managed device. In the device navigation tree, select **Device Admin** to view configuration options.

For more detailed explanation about configuring device administration on security devices, see the “Fundamentals” and “Administration” volumes in the *Concepts & Examples ScreenOS Reference Guide*.

**Related Documentation**


- Importing Device Administrators from a Physical Device Overview on page 31
- Device Administrator Authentication Overview on page 3
- Device Administrator Account Configuration Overview on page 4


## Device Administrator Authentication Overview

To authenticate device administrators when they attempt to connect to the security device, you can use the default authentication server (on the device) or an external authentication server.

The root device administrator is always stored and authenticated using the local database; however, for non-root read/write and read-only device admins (including vsys device admins), you can specify an external auth server (RADIUS, SecurID, or LDAP server) that stores device administrator accounts. To select an external server from the auth server list, you must have already created and configured an Authentication Server object in the NSM UI.

By default, authentication and accounting are performed in the RADIUS auth server. You can configure separate RADIUS servers for accounting and authentication for XAuth and L2TP user types (in ScreenOS 6.2). XAUTH and L2TP users can disable the default accounting and configure a different RADIUS server for accounting.

After the device administrator is authenticated, the auth server checks the privilege level of the device admin. A privilege level defines the privileges that are accessible to the device admin after successful logging in to the device. They are:

- For device administrators stored in the local database, the security device uses the privilege level specified in the local device administrator account.
- For device administrators stored on an external auth server, select one of the following privilege settings:
  - Get privilege from RADIUS server—Select this option to query a RADIUS server for all external device administrator privileges. The RADIUS server must contain the device administrator accounts and netscreen.dct (Juniper Networks dictionary file).
  - Read-Write, Read-Only—Select a privilege level that applies to all external device administrators. Although the device administrator accounts are stored on the external server, the security device provides the device administrator privilege level. Use this option when storing accounts on a SecurID or LDAP server, or when using a RADIUS server that does not contain the Juniper Networks dictionary file. By default, the external device administrator privilege level is set to Read-Only.

**Related Documentation**

- Device Administrator Account Configuration Overview on page 4
- Supporting Admin Accounts for Dialup Connections on page 8
- Importing Device Administrators from a Physical Device Overview on page 31

## Device Administrator Account Configuration Overview

You must create an account for each device administrator on the managed device. The device administrator account contains a device admin privilege level, username, password, and optional PKA keys for the admin.

Additionally, for security devices that run ScreenOS 5.0 or later, you can configure privileges for the Trustee, such as granting the permission to configure the untrust Ethernet interface and the permission to configure the untrust modem interface.

- Configuring Privilege Level on page 4
- Configuring Authentication on page 6
- Admin Access Lock Setting on page 7
- Roles for Device Administrator Accounts on page 7

### Configuring Privilege Level

A security device supports multiple device administrators. NSM connects to the device as the root device administrator, and has complete administrative privileges for the device.

A security device can have only one root device administrator which cannot be deleted. Additionally, after you create the root device administrator (or import from an existing device) you cannot change the name of the root device administrator. To delete an

existing root device administrator, you can change the privilege level of the administrator to a non-root privilege, and then save and delete the administrator. If you delete the root device administrator, however, you must then create a new root device administrator before installing the modeled configuration on the managed device (NSM must use the root device administrator account to communicate with the managed device).

NOTE: For ScreenOS 5.x devices, you can set or change the root device admin password using the directive "Set Root Admin." To execute this directive, right-click the device in the Device Manager device list and select **Device > Set Root Admin**.

When you create other device administrators, you must assign a privilege level; these privileges are accessible to the device admin after successful log in to the device as described in Table 3 on page 5.

*Table 3: Privilege Level*

| Privilege Levels | Description |
|---|---|
| Read/Write Device Administrator | The read/write administrator has the same privileges as the root device administrator, but cannot create, modify, or remove other device administrators. Privileges include:<br>• Creates virtual systems and assigns virtual system administrators<br>• Monitors any virtual system<br>• Tracks statistics (this privilege cannot be delegated to a virtual system administrator) |
| Read-Only Device Administrator | The read-only device administrator has only viewing privileges using the Web UI, and can only issue the **get** and **ping** CLI commands. Privileges include:<br>• Read-only privileges in the root system, using the following four commands: **enter**, **exit**, **get** , and **ping**<br>Read-only privileges in virtual systems<br>NOTE: All system administrators, including those assigned a Read-Only role, can create and run their own reports. |
| Virtual System Device Administrator (available on security devices that support virtual systems) | Each virtual system (vsys) is a unique security domain, which can be managed by virtual system device administrators with privileges that apply only to that vsys. Virtual system administrators independently manage virtual systems through the CLI or Web UI. Privileges include:<br>• Creates and edits auth, IKE, L2TP, XAuth, and Manual Key users<br>• Creates and edits services<br>• Creates and edits policies<br>• Creates and edits addresses<br>• Creates and edits VPNs<br>• Modifies the virtual system administrator login password<br>• Creates and manages security zones<br>• Adds and removes virtual system read-only administrators |

*Table 3: Privilege Level (continued)*

| Privilege Levels | Description |
|---|---|
| Virtual System Read-Only Device Administrator (available on security devices that support virtual systems) | A virtual system read-only administrator has the same set of privileges as a read-only administrator, but only within a specific virtual system. A virtual system read-only administrator has viewing privileges for a particular vsys through the Web UI, and can only issue the **enter**, **exit**, **get**, and **ping** CLI commands within that vsys. |

For any configuration change made by a device administrator, the managed device generates a log entry with the name of the device administrator making the change, the IP address from which the change was made, and the time of the change. These log entries appear as configuration logs in the NSM Log Viewer.

## Configuring Authentication

A device administrator can authenticate a connection to a security device using one of two authentication methods: Password or Public Key (ScreenOS 5.x devices only). However, regardless of the authentication method you want the device administrator to use, you must initially define a password for the admin account. If you later bind a public key to the admin, the password becomes irrelevant.

Use password authentication for device administrators who need to configure or monitor the managed device. You can use this authentication method for device administrators on ScreenOS 5.x devices.

NOTE: **All passwords handled by NSM are case-sensitive.**

- To configure authentication, enter a username, password, and privilege level for the device administrator account, and then select **SSH Password Authentication**.
- To connect using an SSH-aware application, the device administrator (the SSH client) initiates an SSH connection to the managed device (the SSH server). When SSH is enabled on the interface receiving the connection request, the managed device prompts the admin for username and password, and then compares that information to the information in the device admin account. If the username and passwords match, the device authenticates the connection; if they do not match, the device rejects the connection request.

Use Public Key Authentication (PKA) for greater security or to run automated scripts. You can use this authentication method for device administrators on a ScreenOS 5.x device.

- To configure PKA, generate the PKA public/private key pair using the key generate program in an SSH client application (see the SSH client application documentation for more information). The key pair is RSA for SSHv1 and DSA for SSHv2. Assign the private key to the device administrator account, and then load the public key on the managed device using a TFTP server or SSP (ScreenOS 5.1 and later only).
- To connect using an SSH-aware application, the device administrator (the SSH client) initiates an SSH connection to the managed device (the SSH server). When SSH is

enabled on the interface receiving the connection request, the managed device prompts the admin for username and public key (of a public/private key pair), and then compares that information with up to four public keys for that device admin account. If one of the keys matches, the device authenticates the connection; if no keys match, the device rejects the connection request.

When the managed device receives the connection request, it first checks the device administrator account for a public key bound to that administrator. If a matching key is found, the managed device authenticates the administrator using PKA; if no matching key is found, the managed device prompts for a username and password. You can store up to four PKA keys for each device administrator.

You must enable SSH on the interface through which the device administrator connects to the managed device using an SSH connection.

## Admin Access Lock Setting

Admin access lock configuration locks out the administrator who fails to authenticate before the configured timeout from the specified account. If this option is disabled, you cannot set the authentication failure length and the default value is set to 1. If this option is enabled, you can set the admin access locking time to lock out the account. The lockout occurs after the specified number of failed login attempts.

## Roles for Device Administrator Accounts

You can configure role attributes for admin users. If you select the privilege of admin user as root, you cannot set the role attribute (that is, the root administrator cannot set role attributes.) If you set privilege as read-write or read-only, you can assign any of the available role attributes. The default value is Not Assigned.

**Related Documentation**

- Supporting Admin Accounts for Dialup Connections on page 8
- Restricting Management Connections Using Permitted IPs on page 9
- Device Administrator Authentication Overview on page 3

## Supporting Admin Accounts for Dialup Connections

The NetScreen-5XT and the NetScreen-5GT devices support a modem connection for outbound dial-up disaster recovery situations. You can set up trustee accounts for the interface or for the modem. This topic describes the two types of trustees:

- Interface trustee

  An interface trustee has access only to the Untrust interface through the Web UI. An interface trustee can only assign the IP address for the primary Untrust zone interface. Also, an interface trustee account can enable or disable ping responses from an interface. Interface trustees can select either a PPPoE or DHCP client using automatic IP address assignment or a static address assignment client.

- Modem trustee

  A modem trustee can access, configure, and modify only the ISP1 and ISP2 settings. A modem trustee can also test and view the configurations for the ISP3 and ISP4 settings.

You can configure Modem Trustee and Interface Trustee accounts to have Read/Write or Read-Only levels of access.

The connection type to a device by a Trustee administrative account occurs exclusively, preventing any other connection type from occurring. The secure trustee connection prevents local console, Telnet, and SSH sessions to connect to the device if these other connection types attempt to use the trustee's name or password.

**Related Documentation**

- Restricting Management Connections Using Permitted IPs on page 9
- Local Access Configuration Using CLI Management Overview on page 13
- Device Administrator Account Configuration Overview on page 4

CHAPTER 2

# Permitted IPs and General Authentication Overview



## Restricting Management Connections Using Permitted IPs

Use permitted IPs to restrict management connections (a connection in which a device administrator attempts to log in) to specific IP addresses. By default, any host on the trust interface of the managed device can connect to the security device and attempt to log in. You can configure the device to permit management connections from one or more user-defined IP addresses only.

After you create permitted IPs (and update the device with the modeled configuration), the device immediately begins rejecting management connections from nonpermitted IP addresses. If a device administrator is managing the device using a remote network connection and the workstation is not included as a permitted IP, the security device immediately terminates the device administrator's session.

To create a permitted IP, click the **Add** icon in the Permitted IP area, and then configure an IP address and netmask.

NOTE: **Configuring a permitted IP for a device administrator does not affect the NSM–managed device connection.**

Corporation A has a small network in which a single device administrator at 172.16.40.42 is allowed to manage the security device. For this device, you create a permitted IP with an IP/netmask of 172.16.41.42/32.

Corporation B has a large network with multiple devices. Several device administrators on the 172.16.40.0 subnet require access to all devices. For each device, you create a permitted IP with an IP/netmask of 172.16.40.0/24.

On devices running ScreenOS 6.3, permitted IPs used for restricting management connections supports IPv6.

**Related Documentation**

- Local Access Configuration Using CLI Management Overview on page 13
- File Formatting in NSM Overview on page 13
- Supporting Admin Accounts for Dialup Connections on page 8

## Setting ScreenOS Authentication Options Using General Auth Settings

The authentication screens contain the following device-wide authentication options you can configure on a security device.

For devices running ScreenOS 5.2, you can configure some general settings that determine how the security device handles authentication session cleanup and authentication requests.

- Clearing RADIUS Sessions on page 10
- Assigning an Authentication Request Interface on page 10

### Clearing RADIUS Sessions

Occasionally, overcharging can occur when a wireless user is assigned the same IP address that was used for a previously closed connection by a different user. Because the IP addresses are the same for both connections, the first wireless user might be charged for the second user's connection time. You can prevent this problem by configuring the security device to clear RADIUS sessions for a specific IP address when the RADIUS accounting-stop message is received for that connection.

To enable session cleanup for a security device, in the device navigation tree, select **Auth > General**. Configure a RADIUS Accounting Listener port that monitors the connection for accounting-stop messages, and then select the option **RADIUS Accounting Cleanup Action: Session Cleanup**.

### Assigning an Authentication Request Interface

By default, the security device sends authentication requests using the route defined in the route table. For devices running ScreenOS 5.2, you can configure a specific outgoing source interface for requests sent to an authentication server. You might need to specify a specific interface for auth requests destined for a VPN tunnel or to route all auth requests through the same interface for authentication monitoring.

To configure a source interface, in the device navigation tree, select **Auth > General**, and then click the **Add** icon in the Source Interface used for Outgoing Auth Request area. Select the Authentication Server object that represents the authentication server receiving the request, and then select an interface on the device through which requests are sent.

NOTE: For details on configuring Authentication Server objects, see the *Network and Security Administration Guide*.

After you specify a source interface for auth requests, the security device routes all auth requests destined for a RADIUS, LDAP, or SecurID server through that interface (one source interface per authentication server object).

**Related Documentation**

- Setting ScreenOS Authentication Options Using Banners Overview on page 22
- Setting ScreenOS Authentication Options Using Default Servers Overview on page 27
- Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 25

## General Report Settings for ScreenOS Devices Overview

The Report Settings screens contain reporting options that you can set for the device. In the Device dialog box, open the Report Settings heading to see the configuration options.

For information about configuring reporting settings, "General Report Settings for ScreenOS Devices Overview" on page 11.

For more information about reporting concepts for the security devices, see the "Administration" volume in the *Concepts & Examples ScreenOS Reference Guide*.

Use the General Report settings to configure the severity levels of the messages you want to log and where you want those messages sent. As of ScreenOS 6.3, there are about nine destinations for log messages. You can enable or disable the option to include serial numbers in log messages. Each system event on a security device is assigned a level of severity. By default, packets that are dropped on the security device are logged to the self log. In the Firewall Options, you can disable or enable logging of dropped packets for specific traffic types, including ICMP, IKE, SNMP, and multicast packets.

You can also use this tab to set thresholds determining how many packets of a particular type the packet process unit (PPU) sends to the CPU per second, before dropping subsequent packets of that type. The PPU is a hardware processor in some security device systems that forwards packets to the flow CPU. Enabling PPU packet drop thresholds adds an extra layer of DoS-attack protection to the device, similar to SYN-cookie and SYN-proxy. PPU protection prevents DoS attacks from overwhelming the flow CPU, keeping the CPU responsive to critical tasks even under heavy traffic. PPU protection processes three categories of traffic: packets that do not use the IP protocol; packets carrying contents other than TCP or UDP; and system-critical IP packets, including BGP, OSPF, RIP, SNMP, system management, SIP, and H323 traffic. Table 4 on page 11 describes the general report settings.

*Table 4: General Report Settings*

| Report Settings | Function |
|---|---|
| Email Notification Settings | Configures a device to send messages using e-mail whenever a system event of Emergency, Alert, Critical, or Notification severity level occurs. To configure e-mail notification, you must specify the SMTP mail server and at least one e-mail address; if desired, you can enter a secondary e-mail address as well. |

*Table 4: General Report Settings (continued)*

| Report Settings | Function |
|---|---|
| NSM Reporting | Configures a device to report specified events to NSM. You configure the primary IP address of the NSM Device Server and select the categories of events that are tracked on the security device and reported to NSM. You can also set the interval at which the NSM device server polls for policy statistics and protocol distribution events. |
| SNMP Reporting | Configures the Simple Network Management Protocol (SNMP) agent for a device. The SNMP agent provides a view of statistical data about the network, the devices in it, and system events of interest.<br><br>You also must enable SNMP manageability on the interface through which the applicable SNMP manager communicates with the SNMP agent in the security device. |
| Syslog Reporting | Configures a device to generate syslog messages for system events at predefined severity levels. It also generates messages for all event and traffic log entries that the security device can store internally. It sends these messages over UDP (port 514) to up to four designated syslog hosts running on UNIX/Linux systems. When you enable syslog reporting, you also specify which interface the security devices use to send syslog packets. |

**Related Documentation**

- Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 28
- Configuring Syslog Host Using NSM (NSM Procedure) on page 35

CHAPTER 3

# CLI Management Overview



## Local Access Configuration Using CLI Management Overview

Use the CLI management options to configure local access using a console connection, or remote access using Telnet or SSH. A device administrator can connect directly to most security devices using the console port. CLI management settings apply to all device administrators for the security device.

Additionally, to manage a device remotely using Telnet or SSH, the device administrator must use a permitted IP address to initiate a Telnet or SSH connection to the device, and the correct service option must be enabled for the interface that the device administrator connects to on the device. For details on configuring permitted IP addresses, see "Restricting Management Connections Using Permitted IPs" on page 9; for details on configuring service options for a device interface, see the *Network and Security Manager Administration Guide*.

**Related Documentation**

- File Formatting in NSM Overview on page 13
- Port Numbers for SSH and Telnet Connections in NSM Overview on page 14
- Restricting Management Connections Using Permitted IPs on page 9

## File Formatting in NSM Overview

The file format determines the format (DOS or UNIX) of device configuration files. The CLI commands that configure the security device are automatically stored in a text-based

configuration file. Occasionally, for troubleshooting purposes, a device administrator might need to view this configuration file outside of the security device.

To configure the file format of the configuration file, select the format that matches the computer system on which the configuration files will be viewed:

- In a UNIX text file, a line of text is terminated by a line-feed character. When viewing a UNIX text file on a UNIX or DOS-based system, this line feed character does not appear. If you typically view configuration files on a UNIX system, select **UNIX** as the file format.
- In a DOS text file, a line of text is terminated by a line-feed and a carriage return (^M). When viewing a DOS text file on a UNIX system, the carriage return character appears onscreen. If you typically view configuration files on a DOS-based system, select **DOS** as the file format.

**Related Documentation**

- Port Numbers for SSH and Telnet Connections in NSM Overview on page 14
- Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 15
- Local Access Configuration Using CLI Management Overview on page 13

## Port Numbers for SSH and Telnet Connections in NSM Overview

You can configure the port numbers to use for SSH and Telnet connections:

- The default port for SSH client connections is 22; to change this default, enter a port number between 1024 and 32,767.
- The default port for Telnet client connections is 23; to change this default, enter a port number between 1024 and 32,767.

In a vsys system, the root and vsys share the same SSH port number. For example, if you change the SSH port from the default port 22, the port is also changed for all vsys.

NOTE: **For ScreenOS 5.x devices, you can set or change the device port numbers that accept Telnet and/or SSH connections the. "Set Admin Ports" directive. To execute this directive, right-click the device in the Device Manager device list and select Device > Set Admin Ports.**

**Related Documentation**

- Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 15
- Asset Recovery and Reset Hardware in NSM Overview on page 15
- File Formatting in NSM Overview on page 13

## Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview

This topic describes the information about how to limit login attempts, set dial-in authentication, and restrict password length and they are as follows:

**Configuring Connection Attempts**

To minimize unauthorized access, you can limit the number of unsuccessful login attempts allowed before the security device terminates a Telnet session. This restriction also protects against certain types of attacks, such as automated dictionary attacks.

By default, a security device allows up to three unsuccessful login attempts before it closes the Telnet session.

**Configuring Modem Dial-In Authentication Timeout**

You can set dial-in authentication timeout. You can even set the timeout as never time out for users who dialin.

**Configuring Password Length Restriction**

To prevent a root device administrator from using short passwords (which are easier to decode and discover), you can set the minimum length requirement for the root device administrator password to any number from 1 to 31.

However, to set this restriction, the current root device administrator password must meet the minimum length requirement you are attempting to set. If the current password is too short, NSM displays an error message.

**Related Documentation**

- Asset Recovery and Reset Hardware in NSM Overview on page 15
- Console-Only Connections in NSM Overview on page 16
- Port Numbers for SSH and Telnet Connections in NSM Overview on page 14

## Asset Recovery and Reset Hardware in NSM Overview

If the root device administrator password is lost, the device administrator can restore access in one of two ways as described in Table 5 on page 16.

*Table 5: Asset Recovery and Reset Hardware*

| Restore Access Methods | Description |
|---|---|
| Using Asset Recovery | Using a console connection, the device administrator uses the **unset all** command to clear all existing configuration settings and return the device to factory defaults (for details, see the "Administration" volume in the *Concepts & Examples ScreenOS Reference Guide*). Device recovery is enabled by default. To disable it, clear the **Enable Asset Recovery** check box in the CLI Management configuration screen.<br><br>NOTE: A security device in FIPS mode automatically disables asset recovery. |
| Reset Hardware | The device administrator performs a manual operation on the physical device hardware to return the device to factory defaults (for details, see the "Administration" volume in the *Concepts & Examples ScreenOS Reference Guide*). Reset Hardware is enabled by default. To disable it, clear the **Enable Reset Hardware** check box in the CLI Management configuration screen. |

All configuration settings stored on the managed device are lost during an asset recovery or hardware reset. After restoring access to the device, the device administrator should perform the following tasks to enable the device to reconnect to NSM:

1. Configure the interface that connects to the management system.
2. Send the new root device administrator username and password to the NSM administrator, who should update the existing root username and password for the device in the modeled configuration.

NOTE: **All passwords handled by NSM are case-sensitive.**

3. Enable the NSM agent on the managed device.

After the device has reconnected to the management system, you (the NSM administrator) can update the device with the modeled configuration.

**Related Documentation**

- Console-Only Connections in NSM Overview on page 16
- Secure Shell Server in NSM Overview on page 17
- Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 15

## Console-Only Connections in NSM Overview

You can require the root device administrator to log in to the security device through the console port only. This restriction requires the root device admin to have physical access to the device to log in, preventing unauthorized persons from logging in remotely.

By default, this restriction is not enabled (the root device administrator can log in remotely). To restrict access to console only, select the **Root Access Console Only** check box in the CLI Management screen. When enabled, the managed device denies access

to all Web UI, Telnet, or SSH connections for the root device administrator. This setting overrides the management options enabled on the ingress interface.

NOTE: This option does not appear for the Juniper Networks NSM*Xpress*, which does not contain a console port.

Enabling the console-only setting does not affect the NSM–managed device connection.

**Related Documentation**

- Secure Shell Server in NSM Overview on page 17
- Configuring CLI Banners in NSM Overview on page 22
- Asset Recovery and Reset Hardware in NSM Overview on page 15

## Secure Shell Server in NSM Overview

Each security device includes a built-in Secure Shell (SSH) server. Device administrators can use an SSH-aware application to open a remote command shell on the device and execute commands. When using SSH, the connection is protected against IP or DNS spoofing attacks, and password or data interception.

The maximum number of SSH sessions is a device-wide limit and is between 2 and 24, depending upon the device. If the maximum number of SSH clients are already logged into the device, no other SSH client can log in to the SSH server.

To enable SSH connections to the managed device, select **SSH Enable** and configure an SSH version. Because SSHv1 and SSHv2 are incompatible, you must use the same SSH version for both the client and server. For example, you cannot use an SSHv1 client to connect to an SSHv2 server on the managed device, or vice versa.

For the SSH server (the security device), you can also enable Secure Copy (SCP). A device administrator can use SCP to transfer files to or from the managed device using SSH (SSH authenticates, encrypts, and ensures data integrity for the SCP connection). When using SCP, the security device acts as an SCP server that accepts connections from SCP clients on remote hosts. Additionally, you must enable SSH for the managed device before you can enable SCP (disabled by default).

NOTE: For ScreenOS 5.x devices, you can enable or disable SSH for device admin connections using the directive “Set Admin SSH.” To execute this directive, right-click the device in the Device Manager device list and select **Device > Set Admin SSH**.

- Using SSH Version 1 (SSHv1) on page 18
- Using SSH Version 2 (SSHv2) on page 18

## Using SSH Version 1 (SSHv1)

SSHv1 is widely deployed and is commonly used. You can use a password or Public Key Authentication (PKA) to authenticate an SSHv1 connection.

When using PKA authentication for the SSHv1 server (the security device) you can also set the key generation interval for the host PKA key. When you enable SSH on a managed device, the device generates a unique host key that is permanently bound to the device (each vsys has its own host key). If SSH is disabled, then enabled again, the device uses the same host key. The security device uses the host key to identify itself to an SSH client (device administrator).

After the key is generated, it can be distributed to the SSH client in one of two ways:

- Manually—Send the host key to the client admin user through e-mail or phone. The device administrator stores the host key in the appropriate SSH file on the SSH client system (the SSH client application determines the file location and format).
- Automatically—When the SSH client connects to the managed device, the SSH server sends the unencrypted public component of the host key to the client. The SSH client searches its local host key database to see if the received host key is mapped to the address of the security device. If the host key is unknown (there is no mapping to the device address in the client's host key database), the device admin user can accept the host key and authenticate the connection, or reject the host key and terminate the connection request.

To configure the SSH client, you must also bind the RSA PKA keys to the device administrator before that admin can make an SSH connection. For details on assigning PKA keys to a device admin, see "Device Administrator Account Configuration Overview" on page 4.

NOTE: **NSM supports PKA keys for device administrator authentication only for devices running ScreenOS 5.x.**

## Using SSH Version 2 (SSHv2)

SSHv2 is considered more secure than SSHv1 and is currently being developed as the IETF standard.

To configure the SSH client, you must also bind the DSA PKA keys to the device administrator before that admin can make an SSH connection. For details on assigning PKA keys to a device admin, see "Device Administrator Account Configuration Overview" on page 4.

**Related Documentation**

- Configuring CLI Banners in NSM Overview on page 22
- Configuring Remote Access Using Web Management Overview on page 19
- Console-Only Connections in NSM Overview on page 16

CHAPTER 4

# Web Management and Banners Overview



## Configuring Remote Access Using Web Management Overview

Use the Web management options to configure remote access using the Hypertext Transfer Protocol (HTTP). A device administrator can use a standard Web browser and HTTP to remotely access the Web UI on the security device. Web management settings apply to all device administrators for the security device.

Additionally, to manage a device using the Web UI, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the correct service option must be enabled for the interface that the device administrator connects to on the device. For details on configuring permitted IP addresses, see "Restricting Management Connections Using Permitted IPs" on page 9; for details on configuring service options for a device interface, see *Enabling Management Service Options for Interfaces*.

**Related Documentation**

- Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 19
- Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 20
- Configuring CLI Banners in NSM Overview on page 22

## Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview

You can configure the following options for administrative connections that use HTTP:

- Idle time for Web UI management—The number of seconds that the HTTP connection remains idle (no traffic is flowing) before the device drops the connection.

- Port number—The default HTTP port number is 80. If you are running HTTP services on a different device port, enter that port number here.

Additionally, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the Web service option must be enabled for the interface that the device administrator connects to on the device.

To secure HTTP administrative traffic, you can use the Secure Sockets Layer (SSL) protocol.

**Related Documentation**

- Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 20
- Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 25
- Configuring Remote Access Using Web Management Overview on page 19

## Configuring Secure Connections in ScreenOS Devices Using NSM Overview

Secure Sockets Layer (SSL) is a set of protocols that can provide a secure connection between a Web client and a Web server communicating over a TCP/IP network. SSL consists of the SSL Handshake Protocol (SSLHP), which enables a client and server to authenticate each other and negotiate an encryption method, and the SSL Record Protocol (SSLRP), which provides basic security services to higher level protocols such as HTTP. Using certificates, SSL authenticates the server (the security device), and then encrypts the traffic sent during the session. Juniper Networks supports authentication only of the server (the security device), not the client (the device administrator); the device authenticates itself to the device administrator, but the device administrator does not use SSL to authenticate to the device. However, the device administrator must connect using a Web browser with SSL version 3 compatibility (not version 2). Netscape Communicator 4.7x and later and Internet Explorer 5.x and later are SSL version 3 compatible.

During the SSL handshake, the security device sends the device administrator its self-signed certificate. The device admin encrypts a random number with the public key contained in the certificate and sends the number back to the device, which uses its private key to decrypt the number. Both participants then use the shared random number and a negotiated secret key cipher (3DES, DES, RC4, or RC4-40) to create a shared secret key, which they use to encrypt traffic between themselves. They also use an agreed-upon compression method (PKZip or gzip) to compress data and an agreed-upon hash algorithm (SHA-1, SHA-2, or MD5) to generate a hash of the data to provide message integrity.

Additionally, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the SSL service option must be enabled for the interface that the device administrator connects to on the device.

By default, SSL is disabled. To ensure that all HTTP connections to the Web UI are secure, you should enable this option. When enabled, the device automatically redirects administrative traffic using HTTP (default port 80) to HTTPs (SSL, default port 443)

and authenticates using the local certificate. For a device running ScreenOS 5.1 and later, SSL uses the autogenerated, self-signed certificate on the device.

You can change the SSL configuration by editing the SSL settings as described in Table 6 on page 21.

*Table 6: SSL Settings*

| SSL Settings | Your Action |
|---|---|
| Redirect HTTP to HTTPS | You can enable HTTP redirection for SSL troubleshooting, if desired. |
| Certificate | By default, the security device uses an auto-generated self-signed certificate for SSL. To change the certificate used for SSL, select a certificate from the list of available certificates. |
| Port | The default port for SSL connections is 443; to change this default, enter a different port number. |
| Cipher | Select an encryption algorithm for SSL:<br>• RC4-40 with 40-bit keys<br>• RC4 with 128-bit keys<br>• DES: Data Encryption Standard with 56-bit keys<br>• 3DES: Triple DES with 168-bit keys<br>The RC4 algorithms are paired with MD5; DES and 3DES with SHA-1. |
| Authentication | Select an authentication method for SSL:<br>• Message Digest version 5 (MD5)—128-bit keys<br>• Secure Hash Algorithm version 1 (SHA-1)—160-bit keys<br>• Secure Hash Algorithm version 2 (SHA-2)—256-bit keys |

While SSL is enabled, any device administrator can connect to the security device using the SSL port. When administrative connections use SSL, in the Web browser URL field, the device admin must enter the https (instead of http) before the IP address used to manage the device. If you changed the default SSL port from 443, the device administrator must also append a colon and the SSL port number to the IP address. For example, to connect to the 5.5.5.5 interface and SSL port 1443, the device administrator must enter **https://5.5.5.5:1443**.

To use HTTP without SSL, disable SSL by clearing the **Enable SSL** check box. The device no longer redirects HTTP connections to SSL, and no authentication occurs for the connection.

**Related Documentation**

- Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 25
- Setting ScreenOS Authentication Options Using General Auth Settings on page 10
- Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 19

## Configuring CLI Banners in NSM Overview

You can customize the message that appears when a device administrator logs on to the security device using a console connection, Telnet, or SSH. This message, called a banner, provides confirmation to device administrators to let them know that they have successfully logged in. Banners are optional; you are not required to configure CLI banners for the security device.

A default banner already exists for Telnet and SSH, but you can write a new message to suit your needs. You can use one banner for console connection and a different banner for both Telnet and SSH connections.

To configure CLI banners:

- For console connections, enter a message in the Console Login Banner text box. By default, the console banner is blank (no confirmation is provided to the device administrator upon successful login). The maximum number of characters permitted in a console banner is 127.
- For Telnet or SSH connections, enter a new message or edit the existing default message in the Telnet/SSH Login Banner text box. By default, the message “Remote Management Console” is provided to device administrators upon successful login. The maximum number of characters permitted in a Telnet or SSH banner is 127.

For ScreenOS 5.1 and later devices, you can also configure a secondary banner for console, Telnet, or SSH connections. The secondary banner enables you to create a much longer message that appears for any successful CLI-based connection attempt. By default, the secondary banner is blank (no secondary message is provided for device administrators upon login).

In ScreenOS 6.1 , for sessions created through ssh, telnet, or local console, the secondary banner gets displayed after the username and the password prompt. These actions can request the administrator to acknowledge the secondary banner through the CLI console. Hence, if the user does not acknowledge the secondary banner, the device login process fails and the connection is closed.

**Related Documentation**

- Configuring Remote Access Using Web Management Overview on page 19
- Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 19
- Secure Shell Server in NSM Overview on page 17

## Setting ScreenOS Authentication Options Using Banners Overview

You can customize the message that appears when a device user logs on to the security device through Telnet, FTP, HTTP, or WebAuth. This message, called a banner, provides confirmation to device users to let them know the status of the connection. Default banners already exist, but you can write a new message to suit your needs. You can use different banners for each protocol.

NOTE: To configure the Telnet, SSH, or console connection banner, see "Configuring CLI Banners in NSM Overview" on page 22.

To configure a protocol banner, select the protocol tab and edit the default Telnet, FTP, and HTTP messages as described in Table 7 on page 23.

*Table 7: Protocol Banner Settings*

| Protocol Banner Settings | Your Action |
|---|---|
| Attempted Logins | Enter a new message or edit the existing default message in the Login text box. Device users receive this message when they are prompted for their authentication credentials. |
| Successful Logins | Enter a new message or edit the existing default message in the Success text box. Device users receive this message after their credentials have been authenticated and a connection has been established. |
| Failed Logins | Enter a new message or edit the existing default message in the Fail text box. Device users receive this message when authentication fails or when the device user is not authorized to access the device. |

To configure the WebAuth banner, select the **WebAuth** tab and enter a new message (or edit the existing default message in the Success text box. This message is provided to auth user when their WebAuth credentials have been authenticated and a connection has been established. The message appears at the top of a Web browser screen, after an auth user has successfully logged on to a WebAuth address. Typically, the message informs the user that the authentication was successful, but you can enter any message you want, up to a maximum of 220 characters.

Banners are optional; you are not required to configure banners for the security device.

NOTE: Device administrators can create login banners for console, telnet, and secondary connections.

**Related Documentation**

- Setting ScreenOS Authentication Options Using Default Servers Overview on page 27
- Setting ScreenOS Authentication Options Using General Auth Settings on page 10
- Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 28

CHAPTER 5

# Date and Time Management Overview



## Configuring Network Time Protocol and NTP Backup Server in NSM Overview

Use the Date/Time option to configure date and time synchronization on security devices. The date and time setting on the device affects VPN tunnel setup and schedule objects used in active security policies.

You configure the device time in relation to GMT.



### Configuring Network Time Protocol

To ensure that the security device always maintains the right time, the device can use Network Time Protocol (NTP) to synchronize its system clock with that of an NTP server on the Internet.

To use NTP, first enable Network Time Protocol, and then configure the settings as described in Table 8 on page 25.

*Table 8: Network Time Protocol Settings*

| NTP Settings | Your Action |
|---|---|
| Synchronization | You can configure the security device to perform this synchronization automatically at time intervals that you specify. By default, the synchronization interface is set to 10 minutes, with a 3 second maximum adjustment threshold. |

*Table 8: Network Time Protocol Settings (continued)*

| NTP Settings | Your Action |
|---|---|
| Authentication | You can secure NTP traffic by enabling authentication. When using authentication, for each NTP server you configure on the security device, you must assign a unique server key ID and preshare key; the key ID and preshare key serve to create an MD5 checksum, with which the device and the NTP server can authenticate NTP data. Select the authentication mode that the device uses when connecting to an NTP server:<br>• Required—The device must include the authentication information—server key ID and MD5 checksum—in every packet it sends to an NTP server and must authenticate all NTP packets it receives from an NTP server. If authentication fails, the device denies NTP traffic from the NTP server.<br>• Preferred—The device attempts to authenticate NTP traffic using the same methods as the Required options but continues to send and receive NTP traffic if authentication fails.<br>• None (default mode)— Select this mode if you do not want to authenticate NTP packets. |
| NTP Servers | You can configure up to three NTP servers (one primary and two backups) from which the security device can regularly update its system clock. If you enable authentication by selecting the Required or Preferred authentication options, you must also provide a unique server key ID and preshare key for each NTP server that you configure. |

## Configuring an NTP Backup Server

You can specify an individual interface as the source address to direct Network Time Protocol (NTP) requests from the device over a VPN tunnel to the primary NTP server or a backup server as necessary. Among other interface types, you can select a loopback interface to perform this function.

The security device sends NTP requests from a source interface and optionally uses an encrypted preshared key when sending NTP requests to the NTP server. The encrypted preshared key provides authentication.

**Related Documentation**

- Setting ScreenOS Authentication Options Using General Auth Settings on page 10
- Setting ScreenOS Authentication Options Using Banners Overview on page 22
- Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 20

CHAPTER 6

# Default Servers and Infranet Settings Overview



## Setting ScreenOS Authentication Options Using Default Servers Overview

The default servers for the security device define the authentication servers used to provide local, external, and WebAuth user authentication. Table 9 on page 27 describes the different default servers.

*Table 9: Default Servers*

| Default Servers | Description |
|---|---|
| Local | Each security device contains a local (database) server called auth server. The auth server is the default authentication server and can handle all types of authentication that occur on the device. Usernames and authentication credentials of all local users are stored in this database.<br><br>For the Local server only, you can set the authentication timeout, which is the number of minutes the connection remains active after an authentication request has been submitted and a successful authentication is received. By default, the authentication timeout on the Local authentication server is 10 minutes. To change this timeout, enter a new value. |
| External | Alternatively, you can select an external authentication server as the default server. To select an external server, you must have already created and configured an Authentication Server object in the NSM UI. You must also have defined the user accounts for all external users on the external server. For more information, see the *Network and Security Manager Administration Guide*. |
| WebAuth | When using WebAuth, an auth user first initiates an HTTP session to the IP address of the security device that hosts WebAuth. After successful authentication, the auth user can send traffic to the destination as permitted by one or more security policies. To authenticate WebAuth users, you can use the Local authentication server (security device default) or select a previously defined external auth server. |

**Related Documentation**

- Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 28

- General Report Settings for ScreenOS Devices Overview on page 11
- Setting ScreenOS Authentication Options Using Banners Overview on page 22

## Setting ScreenOS Authentication Options Using Infranet Settings Overview

If you have deployed Juniper Networks Infranet Controllers as part of your network security infrastructure, you can use the Infranet Settings screen on devices running ScreenOS 5.3 and later to configure the properties as described in Table 10 on page 28.

*Table 10: Infranet Settings*

| Infranet Settings | Description |
|---|---|
| Contact Interval | The time interval (in seconds) that the Infranet Enforcer waits before attempting to connect to the next available Infranet Controller; the default interval is set to 10 seconds. |
| Action on Timeout | For any reason, if your connection to the Infranet Controller times out, the device terminates the SSH connection and clears all Infranet Controller related context. You can change this behavior by setting the timeout action to "Open," in which case the Infranet Enforcer allows all traffic; or "No Change," in which case the Infranet Enforcer preserves the current state of all existing tunnel sessions. |
| Enforcer Mode | This setting takes the Infranet Enforcer out of regular mode and into Test mode. Test mode is recommended before you actually deploy the Infranet Enforcer enabling you to evaluate how the solution works. In this mode, the Infranet Enforcer allows all traffic that matches the Infranet policy. Logs are created indicating the behavior of the Infranet Enforcer as if it were operating in Regular mode. |
| Infranet Controllers | You can configure up to eight (8) Infranet Controllers. The order in which these are entered is used by the Infranet Enforcer to contact each Infranet Controller. Devices permit only one redirect URL per Infranet Controller.<br><br>In devices running ScreenOS 6.2 or later, when UAC is deployed through a ScreenOS firewall, the firewall acts as the Infranet Enforcer and redirects unauthorized access to a configured URL (captive portal). The device configures the redirect URL through a policy, which means that more than one redirect URL can be configured for the same Infranet Controller. |

You can also configure security devices to authenticate using Infranet Controllers in a rule in a security policy. Refer to the *Network and Security Manager Administration Guide* for more information.

**Related Documentation**

- General Report Settings for ScreenOS Devices Overview on page 11
- Configuring Syslog Host Using NSM (NSM Procedure) on page 35
- Setting ScreenOS Authentication Options Using Default Servers Overview on page 27

PART 2

# Integration

CHAPTER 7

# Integration of Advanced Network Settings



## Importing Device Administrators from a Physical Device Overview

A device administrator is the person responsible for managing a device locally using ScreenOS (command line or Web UI). A security device includes one default device administrator account, the root device administrator, which has complete access to all functionality on the device. Using the Network and Security Manager (NSM), you can create 20 additional device administrators with different privilege levels.

NOTE: **To enable a device administrator to use NSM to manage devices, you must create an NSM administrator account for the device admin. For details, see *Network and Security Manager Administration Guide*.**

When you import a device configuration into NSM, device administrator accounts are not automatically imported—you must manually import the accounts from the device using a separate directive. You cannot manage device administrator functionality in NSM until you have imported the device administrator information from the physical device (the device admin screens do not appear).

To notify you when device administrator information needs to be imported, NSM displays the message "Need to Migrate Admin Info From Device." To view this message, in the device navigation tree, select **Device Administration**; the message appears in the main display area. When present, this message indicates that you have not yet imported device administrators for that device. This message automatically appears after you perform the following operations:

- Adjust the ScreenOS version—For details, see *Network and Security Administration Guide*.

To import device administrator information, from the File menu, select **Devices > Configuration > Import Admins**.

NOTE: **The Import Admin directive lists only ScreenOS devices.**

**Related Documentation**

- Device Administration Options for ScreenOS Devices Overview on page 3
- Device Administrator Authentication Overview on page 3
- Device Administrator Account Configuration Overview on page 4

PART 3

# Configuration

CHAPTER 8

# Configuration of Advanced Network Settings

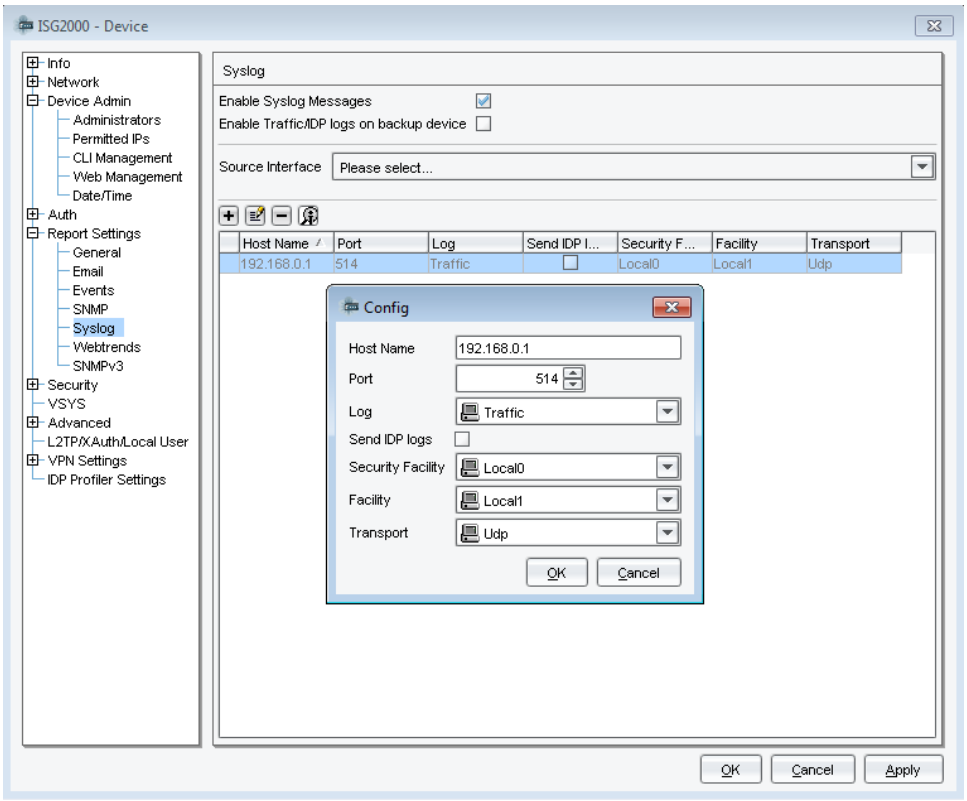


## Configuring Syslog Host Using NSM (NSM Procedure)

To configure syslog hosts using NSM:

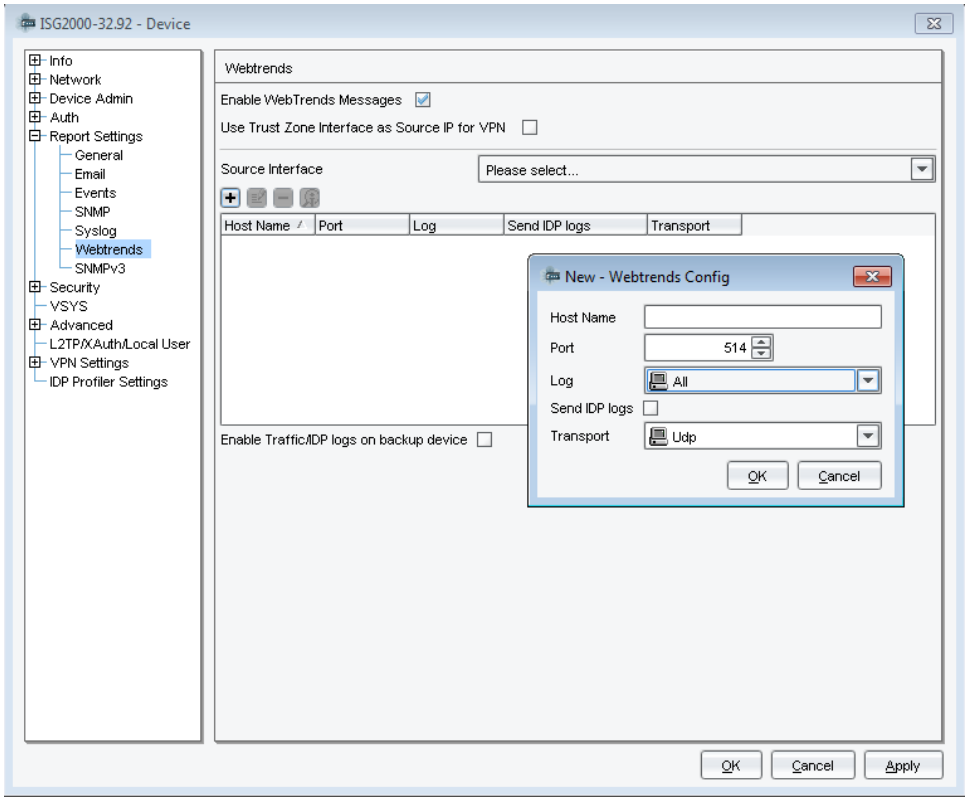
1. Click the **Add** icon in the Syslog configuration screen. The host configuration dialog box appears as shown in Figure 1 on page 36.

*Figure 1: Syslog Configuration Screen*




2. Specify the hostname and the port to which the security device sends syslog messages.
3. For each syslog host, you specify the following:
   - Whether the security device includes traffic log entries, event log entries, or both traffic and event log entries
   - The security facility, which classifies and sends messages to the Syslog host for security-related actions; and the regular facility, which classifies and sends messages for events unrelated to security
   - Which transport protocol (UDP or TCP) is used for sending syslog messages
4. Click **OK**.
5. Use WebTrends reporting to configure a device to send syslog reports to a WebTrends Syslog host. WebTrends Firewall Suite enables you to customize syslog reports to display the information you want in a graphical format as shown in Figure 2 on page 37.

*Figure 2: WebTrends Reporting Screen*




To configure the security device to send syslog reports to a WebTrends Syslog host, you first enable WebTrends reporting, and then specify the name of the WebTrends host and the port on which the syslog messages are sent. If you are sending reports through a VPN tunnel, click **Use Trust Zone Interface**.

As of ScreenOS 6.3, the event log, traffic log, and IDP log formats follow the WebTrends Enhanced Format (WELF) log regulation. If backup for the logs is enabled, logs can be sent to a maximum of four WebTrends servers. TCP or UDP transport protocol can be used for communication. IP connections can be manually reset.

For more details on configuring these reporting options, see the *Network and Security Manager Administration Guide*.

**Related Documentation**

- Configuring SNMPv3 in ScreenOS Devices (NSM Procedure) on page 37
- General Report Settings for ScreenOS Devices Overview on page 11

## Configuring SNMPv3 in ScreenOS Devices (NSM Procedure)

The Simple Network Management Protocol (SNMP) agent for a Juniper Networks security device provides network administrators with a way to view statistical data about the network and the devices on it and to receive notification of system events of interest.

Juniper Networks security devices support SNMPv1, SNMPv2c, and SNMPv3. Security devices are not shipped with a default configuration for SNMPv3. To configure your security device for SNMPv3, you must first create a unique engine ID to identify an SNMP entity and a user-based security model (USM) with the respective privilege and password. By default, the SNMPv3 engine ID is the serial number of the device.

When you create a USM, you can specify the authentication type (MD5, SHA, or None). The authentication type computes identical message digests for the same block of data. The USM requires a password and uses Data Encryption Standard (DES) to encrypt and decrypt the SNMPv3 packets.

To configure SNMPv3 features in ScreenOS devices:

1. In the NSM navigation tree, select **Device Manager > Devices**. The Device Tree page appears.
2. Click the **Device Tree** tab, and then double-click the security device for which you want to configure SNMPv3 features.
3. In the Configuration page, select **Report Settings > SNMPv3**. The SNMPv3 page appears.
4. Add or modify the SNMPv3 features as described in Table 11 on page 38.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

*Table 11: Configuring SNMPv3 Features in ScreenOS Devices*

| Option | Description |
|---|---|
| SNMPv3 > Basic tab | |
| Local Engine ID | Identifies an SNMP entity and a USM with the respective privilege and password. |
| SNMPv3 > USM User tab | |
| User Name | Specifies the username of the USM. |
| Auth Protocol | Specifies an authentication type. Select a value from the drop-down list. When you select either MD5 or SHA, you are prompted to enter an authentication password. |
| SNMPv3 > View tab | |
| View Name | Specifies the view name of the model. Each view is tagged with an object identifier (OID) and mask values. |
| Oid | Specifies the object identifier. The format to enter an OID: Begin with "." and separate by ".". For example, *.3.4.5.2* |
| Mask | Specifies the mask values of the view model. You can enter a two-digit value only. |

*Table 11: Configuring SNMPv3 Features in ScreenOS Devices (continued)*

| | |
|---|---|
| Type | Specifies if you want to include or exclude an IP address entry from the address list of the MIB tables. |
| **SNMPv3 > Access Group tab** | |
| Group | Specifies the access group name. |
| Security Model | Specifies the security model for the access group. |
| Security Level | Specifies the security level for the access group. |
| Notify | Specifies the notification parameter for the access group. |
| Read | Specifies the read access privilege for the access group. |
| Write | Specifies the write access privilege for the access group. |
| **SNMPv3 > Community tab** | |
| Community Name | Specifies the community name that is in combination with an access group. |
| Tag | Specifies the tag name. Each community is tagged. |
| **SNMPv3 > Sec-to-group Mapping tab** | |
| Group | Specifies the group name of the group section map. |
| Security Model | Specifies the security model of the group section. |
| Mapping User | Specifies the username that is mapped with the USM. |
| **SNMPv3 > Filter tab** | |
| Filter Name | Specifies the filter name. A security device can support up to 32 SNMPv3 filters. |
| Oid | Specifies the object identifier. The format to enter an OID: Begin with "." and separate by ".". For example, *.3.4.5.2* |
| Mask | Specifies the mask values of the filter. You can enter a two-digit value only. |
| Type | Specifies if you want to include or exclude an IP address entry from the address list of the MIB tables. |
| **SNMPv3 > Target Parameter tab** | |
| Target Parameter Name | Specifies the target parameter name that is used while sending a trap to a target. A security device can support up to 32 target parameters. |
| Filter | Specifies the filter that you have created. Each filter is tagged to a target (host). |
| Security Model | Specifies the security model of the target parameter. |
| Security Level | Specifies the security level of the target parameter. |

*Table 11: Configuring SNMPv3 Features in ScreenOS Devices (continued)*

| | |
|---|---|
| Community | Specifies the community that you have created. |
| **SNMPv3 > Target Address tab** | |
| Target Name | Specifies the target name. |
| IPv4/IPv6 Address | Specifies either the IPv4 or IPv6 IP address. The system sends the trap to the target if the mask is 32 for IPv4 addresses or 128 for IPv6 addresses. |
| Netmask/Prefix | Specifies the netmask of the IPv4 or IPv6 IP address. |
| Port | Specifies the port. |
| Target Parameter | Specifies the target parameter that you have created. |
| Tag List | Specifies the tag value that you have selected in the filter. |

**Related Documentation**

- General Report Settings for ScreenOS Devices Overview on page 11
- Device Administration Options for ScreenOS Devices Overview on page 3