Revision A

McAfee Network Security Platform 10.1

(FIPS Certification and Common Criteria Compliance Guide)

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

Conventions

This guide uses these typographical conventions and icons.

Italic	Title of a book, chapter, or topic; a new term; emphasis
Bold	Text that is emphasized
`Monospace`	Commands and other text that the user types; a code sample; a displayed message
Narrow Bold	Words from the product interface like options, menus, buttons, and dialog boxes
Hypertext blue	A link to a topic or to an external website
	**Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
	**Tip:** Best practice information
	**Caution:** Important advice to protect your computer system, software installation, network, business, or data
	**Warning:** Critical advice to prevent bodily harm when using a hardware product

What's in this guide

This document is specially designed to cover features and enhancements in Network Security Platform for Federal Information Processing Standard (FIPS) 140-2 and Common Criteria certification.

Find product documentation

Network Security Platform Documentation can be accessed using one of the two options listed below:

1 McAfee Documentation Portal: To view the documents, perform the following steps:

   a Go to McAfee Documentation Portal (https://docs.mcafee.com/).

   b Scroll to the **Products A-Z** section in the landing page.

   c Click **Network Security Platform/Virtual Network Security Platform**.

   The **Network Security Platform/Virtual Network Security Platform** documentation list is displayed.

   d To view documentation for a particular version, use the **Product** filter in the left pane.

2 McAfee Download Server: PDF versions of the product documentation provided alongside this release.

   a Go to the **McAfee Download Server** at https://secure.mcafee.com/apps/downloads/my-products/login.aspx.

   b Enter the **Grant Number** and **Email Address**.

   c Click **Submit**.

   d Under the **Filters** in the left pane, select **Network Security**.

   e Click on the product name for the version of your choice.

   f Under the **Filters** in the left pane, select **DOCUMENTATION**.

   g Download the .ZIP file that contains the documentation for the product.

1 An overview of Network Security Platform

McAfee® Network Security Platform combines McAfee Network Security Sensor (Sensor) and McAfee Network Security Manager (Manager) for the accurate detection and prevention of known attacks using signature detection, zero-day attacks using anomaly detection, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks.

Sensors can be deployed in a variety of topologies such as SPAN or Hub, Tap, In-line fail-closed, and In-line fail-open. Additionally, Sensors support features like interface groups or port clustering where multiple ports on a single Sensor can be grouped together for effective traffic monitoring, particularly useful for asymmetrically routed networks. Network Security Platform also provides high-availability that is, if one Sensor fails, then the standby Sensor automatically takes over and continues to monitor the traffic with no loss of session state or degradation of protection level. A high-availability solution, called Manager Disaster Recovery (MDR), is available for the Manager as well.

The following are the currently available NS-series Sensor models for IPS/IDS: NS9500, NS9300, NS9200, NS9100, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3500, NS3200, and NS3100.

Contents

Overview

The information in this document supplements that released in the Network Security Platform 10.1 user documentation.

This document covers enhancements that are supported in the following versions of Network Security Platform software:

- Network Security Manager software version: 10.1.19.x
- Signature set: 10.8.x.x
- NS-series Sensor software version: 10.1.17.x

The Manager in this release can be run using two modes:

- Non-FIPS mode: All Manager features up to 10.1 are supported in the non-FIPS mode.
- FIPS mode: All features supported in this mode are FIPS compliant:
  - The Manager version that supports FIPS can manage both FIPS and non-FIPS Sensors.
  - The Central Manager and MDR features can be used in this mode but are not FIPS compliant.

- The Manager and Sensor version supports features that are mandatory requirement for Common Criteria certification.
- The new features are certified for Common Criteria for Manager Appliance Linux and NS-series Sensors.

Sensor features in FIPS compliant images

The algorithms implemented in the Sensor image are FIPS 140-2 compliant. Make note of the following features when FIPS compliant images are enabled in the Sensor:

For a list of Sensor features that do not specifically relate to FIPS mode, refer to *McAfee Network Security Platform 10.1.x Product Guide*.

- The Sensor version supports features that are mandatory requirement for Common Criteria certification.
- This FIPS Sensor image only permits the subsequent load of a SHA-256 signed Sensor image. This is mandated by FIPS 140-2, effective 2014. A subsequent load of a Sensor image signed using a weaker algorithm (for example, sha1WithRSAEncryption) fails. You must `netboot` the Sensor to load a non-FIPS image signed with a weaker algorithm.
- All critical security parameters (CSPs) are zeroized, in compliance with FIPS 140-2.
- The following channels operate with algorithms approved by FIPS 140-2:
  - Alert Channel
  - Log Channel
  - Authentication Channel

  The SNMPv3 channel between the Manager and Sensor uses AES128 encryption, SHA authentication, and is RFC3414 and RFC3826 compliant. All CSP information on this channel is additionally encrypted by the Manager using the Sensor 2048-bit RSA and can be decrypted only by the Sensor private key.
- Common Criteria compliance requires the use of specific secure protocols. Hence SNMPv3 is further encapsulated within TLS. The Sensor will use port 18500 as a TLS server for this service.

  If the trust between the Manager and Sensor is established using a self-signed certificate, the Sensor will use port 8500 to service SNMPv3 as a TCP/UDP server. If the trust between the Manager and Sensor is established using a CA-signed certificate, the Sensor will use port 18500 to service SNMPv3 as a TLS server.
- The Sensor alert, packet log, and authentication channels use TLS_ECDHE_RSA_AES128_GCM_SHA256.
  - The Sensor supports read-only access to third party SNMPv3 clients. Third party SNMPv3 clients can only be configured at the Manager. The Sensor retains the use of port 8500 for SNMPv3 service to these clients.
- TACACS+ authentication configuration is disabled at the Sensor level.
- Stronger authentication for user login enforced.
- The Manager version that supports FIPS can manage Sensors that are not FIPS compliant. In the Common Criteria (CC) evaluated configuration, all Sensors must be in FIPS mode.
- When a Sensor of a fail-over pair is running a FIPS image, it is mandatory for the peer Sensor to also be FIPS compliant.

  Before you upgrade convert the Sensors in the fail-over pair to standalone Sensors. If you do not do this trust will not be re-established after the upgrade.

- The channels use RSA certificates based on 2048-bit RSA keys.
- Use SCP for file transfers. The use of TFTP is not permitted.
- Cryptographic support is provided by McAfee modified OpenSSL-Fips-Object-Module v2.0.5 along with OpenSSL v1.0.2m.
- McAfee modified OpenSSH v7.6p1 is configured to support only:
  - Ciphers: aes256-gcm, aes128-gcm
  - MACs: hmac-sha2-256 and hmac-sha2-512
  - KexAlgorithms: ecdh-sha2-nistp256
  - HostKeyAlgorithms: ecdsa-sha2-nistp256
- SSH in 10.1 FIPS Sensor image is restricted to AES GCM Mode cipher only. The use of AES CBC or CTR mode is not permitted.
- This requires that an external SSH client or server must support AES GCM mode ciphers. Some popular clients (like PuTTY) may not support them currently. In such scenarios, you must migrate to an alternative SSH client or server approved by your local administrator.
- The external SSH client is used to log into a Sensor running 10.1 FIPS image.
- The external SSH server is used to host a remote Sensor image, that you can SCP into the Sensor running a 10.1 FIPS image using the `loadimage` CLI command.

Protocol features in the certified evaluated configuration

Usage of NTP is not permitted. The system time may be configured by authorized administrators via the “date” command of the CLI.

The TLS functionality of the NSP components is pre-configured and fixed with the following behaviors:

- Only TLS v1.2 is supported
- The reference identifier is the IP address or fully qualified domain name of the configured endpoint (matching the type used to configure the endpoint) and may be found in the SAN or CN fields of the presented certificate.
- The management GUI interface on the Manager supports the following cipher suite:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- The interface on the Manager supports secp256r1 and secp384r1 Elliptic Curve Extensions.
- Between Sensors and the Manager, the cipher suite used to perform mutual authentication is TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. The systems must use CA-signed RSA certificates with key size 2048 bits.
- The syslog server interface on the Manager supports the following cipher suites:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

2 Upgrade Paths

This section mentions the various upgrade paths available to migrate to latest FIPS mode Network Security Manager. It takes into consideration, several scenarios to migrate to a FIPS-supported version of Network Security Platform 10.1. For a list of upgrade paths not related to FIPS mode, refer to the *McAfee Network Security Platform 10.1.x Installation Guide*.

Migrating the Manager

This section shows you different scenarios of deployment from which you can migrate to the latest FIPS mode Network Security Manager.

You can log in to the McAfee Download Server using your Grant ID to verify the file hash for the software build.

Table 2-1 Manager migration paths

Current Manager version	Intended Manager version
9.1.19.32, 9.1.21.33	10.1.19.x
8.1.19.23, 8.1.19.29, 9.1.21.33	10.1.19.x

Table 2-2 Manager upgrade paths

Manager version	Recommended Manager version
8.1.19.18, 8.1.19.19, 8.1.19.23, 8.1.19.29	10.1.19.x
9.1.19.6, 9.1.19.7, 9.1.19.32	10.1.19.x
9.1.21.20, 9.1.21.33, 9.1.21.38	10.1.19.x

Upgrade from non-FIPS Manager to FIPS Manager in FIPS mode or FIPS Manager in non-FIPS mode is not supported.

Adding FIPS compliant and non-compliant Sensors

You can add both FIPS compliant and non-FIPS compliant NS9500/NS9x00/NS7x00/NS7x50/NS5x00/NS3500/NS3x00 series Sensor models to the Manager. The table below shows the upgrade scenarios for different Sensor versions.

Sensor upgrade path

Upgrade to the mandatory 10.1 FIPS Sensor image is supported through the upgrade paths mentioned in this section.

Table 2-3 Sensor upgrade paths

Sensor model	Current Sensor software (FIPS compliant)	Upgrade path to latest FIPS compliant Sensor software
NS9x00, NS7x00, NS5x00, NS3x00 series	8.1.17.30, 8.1.17.32, 8.1.17.33, 8.1.17.34	10.1.17.x
NS9x00, NS7x50, NS7x00, NS5x00, NS3x00 series	9.1.17.2, 9.1.17.4, 9.1.17.100, 9.1.17.104, 9.1.17.105	10.1.17.x

This is the first certified software images for NS9500 and NS3500 Sensor. Hence, upgrade is not applicable for these Sensor models.

The following applies for FIPS software running on NS-series Sensors:

- The user must synchronize a symmetric key, specified from the CLI using the `set fips sharedkey` command, on both the Primary and Secondary Sensors of an NS9300.
- The Sensor bootloaders are automatically upgraded to allow verification of subsequent image downloads signed with SHA256. Refer to KB85240.
- The FIPS Sensor boot-up executes all the FIPS compliant algorithms, as part of the power-on self-tests (POST) and known answer tests (KAT).

3 Sensor CLI for Certification

Contents

SSH public key based authentication for Sensor

You can use SSH public key authentication or password based authentication to login to the Sensor/remote machine using SSH. Use of public key authentication allows administrators and users to access the Sensor or the remote machine without the use of password based authentication.

Sensor as the SSH server

You can access the Sensor remotely using SSH from a remote machine. The SSH public key from the remote machine has to be configured in the Sensor. Since the Sensor does not permit any key to be exported by the remote client, you must import the key explicitly for every user.

The steps to access Sensor through SSH from a remote machine is as follows:

1. Generate the key pair (SSH public and private keys) for a user accessing the Sensor through a remote machine.
2. Add the user to the Sensor using `adduser` CLI command.
3. Set SCP server IP address from where the SSH public key is to be imported to the Sensor to login.
4. Import your SSH public key to the Sensor using the `importsshpublickey` CLI command.
5. Sensor updates the SSH local repository with the SSH public key.
6. When you login to the Sensor using the SSH key, the Sensor authenticates the user with the SSH public key stored in the local repository.

Sensor as the SSH client

You can SCP files to a remote machine serving as a SCP server from the Sensor. This requires the Sensor SSH public key to be configured on the remote SCP server for the user. The Sensor exports this key to the remote SCP sever if permitted to do so.

The steps to configure Sensor's ssh public key on remote machine are as follows:

1 The Sensor generates a public-private key (ECDSA) pair using the SSH utility "ssh-keygen".

2 The Sensor retains the private-key and exports the SSH public key to the remote machine using `exportsshpublickey` CLI command.

> The `exportsshpublickey` CLI command exports the Sensor's SSH public key to the configured scp server.

> The `exportsshpublickey` CLI command exports the Sensor's SSH public key to the remote machine only by password based authentication.

There are two outcomes while executing `exportsshpublickey` cli command:

- When the public key of the Sensor is directly configured on the remote machine:

```
IntruDbg#> exportsshpublickey <path>

Please enter the SCP User Name : emb-demo

Please enter the SCP User Password :

Public Key configured on the remote machine
```

  In this scenario, the Sensor successfully configures the SSH public key on the remote machine.

- When the public key is not configured but just copied on the remote machine:

```
IntruDbg#> exportsshpublickey <path>

Please enter the SCP User Name : emb-demo

Please enter the SCP User Password :

Transfer Successful through scp, User need to configure the public key manually
on the remote machine.
```

  In this scenario, the Sensor fails to configure the SSH public key on the remote machine, but a copy of it is saved in the file path provided (`<path>`) in the remote machine. You need to manually configure the SSH public key on the remote machine's *authorized_keys* file.

> If the SSH public key authentication fails, the Sensor reverts back to password based authentication method.

> The SSH public key authentication could fail due to incorrect permission of authorized keys, change the mode of `authorized_keys` file to 600 and try again.

Sensor CLI commands related to Certification

The following CLI commands support the mandated requirements for FIPS and Common Criteria certification and can be used on a FIPS and Common Criteria compliant Sensor. However, for a list of commands that can be used in other modes of operation and their availability for different roles, refer to the *McAfee Network Security Platform 10.1.x Product Guide*.

auditlogupload

Uploads the audit log file to the configured SCP server.

Syntax:

```
auditlogupload scp WORD
```

where `WORD` stands for the name of the audit log file to be uploaded.

Note the following:

- For NS-series Sensors, when loading the audit log file to the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor will revert to password authentication.

  For NS-series Sensors, even if the public key authentication is not configured on the Sensor, the first login attempt will be using the public key. If the SSH public key is not present, a warning message will be displayed and the Sensor will then revert to password based authentication.

- When loading an audit log file on the SCP server, you are prompted for the SCP server credentials. The command succeeds only on providing the correct SCP server credentials.

  If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

- When loading an audit log file on the SCP server the pathname of the file should be absolute.

Applicable to:

NS-series Sensors

auditlog remove

Removes auditlog file on the Sensor.

Syntax:

```
auditlog remove
```

Applicable to:

NS-series Sensors

deinstall

Clears the Manager-Sensor trust data (the certificate and the shared key value). Every time you delete a Sensor from the Manager, you must issue this command on the Sensor to clear the established trust relationship before reconfiguring the Sensor.

This command has no parameters.

Syntax:

```
deinstall
```

On executing the command, if the Sensor has CA-signed certificate, the following messages are displayed:

```
Do you want to retain the current CA signed certificate chain ?

Enter Y/y(for yes) or N/n(for no): Y
```

If you enter **Y**, the CA-signed certificate chain for the Sensor is retained. If you enter **N**, both the current Sensor CA-signed certificate and self-signed certificate will be removed along with the trust.

Pressing **Y** displays the following message:

```
deinstall the sensor and remove the trust with the manager ?
```

```
Please enter Y to confirm: Y
```

If you enter **Y**, the Manager-Sensor trust is removed. If you enter **N**, the Manager-Sensor trust remains intact and you exit the deinstall prompt.

```
deinstall in progress ...

this will take a couple of seconds, please check status on CLI
```

On executing the command, if the Sensor has self-signed certificate, the following messages are displayed:

```
deinstall the sensor and remove the trust with the manager ?

Please enter Y to confirm: Y
```

If you enter **Y**, the Manager-Sensor trust is removed. If you enter **N**, the Manager-Sensor trust remains intact and you exit the deinstall prompt.

Entering **Y** displays the following message:

```
deinstall in progress ...

this will take a couple of seconds, please check status on CLI
```

Applicable to:

NS-series Sensors

loadconfiguration

Loads the Sensor configuration from the configured SCP server. The SCP server IP is specified in the Sensor. When the Sensor is added to the Manager, the configuration type should be specified as offline.

Syntax:

```
loadconfiguration scp WORD
```

where `WORD` stands for the name of the configuration file on the SCP server.

Note the following:

- For NS-series Sensors, when loading Sensor configuration from the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor will revert to password authentication.
- When loading Sensor configuration from the SCP server, you are prompted for the SCP server credentials (username and password). The command succeeds only on providing the correct SCP server credentials.

  If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

- When loading Sensor configuration from the SCP server, the pathname of the file should be absolute.

Applicable to:

NS-series Sensors

loadimage

Loads a Sensor image file from the configured SCP server.

Syntax:

```
loadimage scp WORD
```

where `WORD` stands for the name of the image file on the SCP server.

Note the following:

- For NS-series Sensors, when loading a Sensor image file from the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor will fall back to the password authentication.
- When loading a Sensor image file from the SCP server, you are prompted for the SCP server credentials (username and password). The command succeeds only on providing the correct SCP server credentials.

  If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

- When loading a Sensor image file from the SCP server, the pathname of the file should be absolute.

Applicable to:

NS-series Sensors

resetconfig

Resets all configuration values to their default values. It deletes or resets values as described in the following table. This command causes an automatic reboot of the Sensor.

Deleted Values	Values Reset to Defaults
• Manager address (and secondary interface's IP address, if configured). This can be IPv4 or IPv6 address.	• Monitoring and Response port settings
• Certificates establishing trust between Sensor and Manager (shared key value)	• Management port settings
• Signatures	• Manager Install port value
• TFTP server IP address (IPv4 or IPv6 address)	• Manager Alert port value
• SCP server IP address (IPv4 or IPv6 address)	• Manager Log port value
• DoS profile files (learned DoS behavior)	
• SSL Key	
• Exception Object	
• ACL	
• Advanced Setting	

On executing the command, if the Sensor has CA-signed certificate, the following messages are displayed:

```
Do you want to retain the current CA signed certificate chain ?

Enter Y/y(for yes) or N/n(for no): Y
```

If you enter **Y**, the CA-signed certificate chain for the Sensor is retained. If you enter **N**, both the current Sensor CA-signed certificate and self-signed certificate is removed along with the trust.

Pressing **Y** displays the following message:

```
Reset other configurations and reboot? Please enter Y to confirm: Y
```

If you enter **Y**, the Manager-Sensor trust is removed. If you enter **N**, the Manager-Sensor trust remains intact and you come out of the deinstall prompt.

Pressing **Y** displays the following message:

```
resetting the configuration and rebooting the sensor
```

On executing the command, If the Sensor has self-signed certificate, the following messages are displayed:

```
reset the configuration and reboot? Please enter Y to confirm: Y
```

Entering **Y** displays the following message:

```
resetting the configuration and rebooting the sensor
```

Syntax:

```
resetconfig
```

Applicable to:

NS-series Sensors

sshlogupload

Use this command to upload the SSH log file to the SCP Server.

Ensure the following before using this command:

- The SCP server IP address must be set using the command `set scpserver ip <server_ip>`.

The file uploaded on the SCP server is the TAR file containing one or more zipped files:

- Untar the file using the command `tar -xvf <filename>` to get the individual zipped files.
- Each file must be unzipped using the command `gunzip <zipped_file>` to view the file.
- For NS-series Sensors, when loading the SSH log file to the SCP server, the first attempt will be based on SSH public key authentication. If that fails the Sensor will fall back to the password authentication. If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

Syntax

```
sshlogupload scp word
```

A sample SSH log message is displayed below:

```
Sep 16 09:09:52 localhost kernel: SSHD_DROP:IN=eth0 OUT=
MAC=00:06:92:25:9d:80:00:0b:bf:a1:b7:fc:08:00 SRC=172.16.232.47
DST=172.16.199.89 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=4286 DF
PROTO=TCP SPT=2821 DPT=22 WINDOW=65535 RES=0x00 SYN URGP=0
```

SSH log only contains entries for SSH accept or SSH drop from a particular client IP address as defined in the ACL.

Log Message Fields	Description
SSHD_DROP	The Log prefix. It can be SSHD_DROP or SSHD_ACCEPT.
IN=etho	Interface the packet was received from. Empty value for locally generated packets.
OUT=	Interface the packet was sent to. Empty value for locally received packets

Log Message Fields	Description
MAC=00:06:92:25:9d: 80:00:0b:bf:a1:b7:fc:08:00	The MAC field consisting of 14 entities, separated by colons, and this can read as: • **Dest MAC= 00:06:92:25:9d:80** - The destination MAC address. • **Src MAC=00:0b:bf:a1:b7:fc** - The source MAC address. • **Type=08:00** - Ethernet frame carrying an IPv4 datagram.
SRC=172.16.232.47 DST=172.16.199.89	Source IP address Destination IP address
LEN=48	The total length of IP packet in bytes.
TOS=0x00 PREC=0x00	The Type Of Service, “Type” field. The Type Of Service, “Precedence” field.
TTL=127	The remaining Time To Live is 127 hops.
ID=4286 DF	The unique ID for this IP datagram, shared by all fragments if fragmented. Do not Fragment flag.
PROTO=TCP	The protocol name.
SPT=2821 DPT=22 WINDOW=65535	The source port The destination port The number of bits specified on the “Window Scale” TCP option.
RES=0x00	The reserved bits
SYN URGP=0	The synchronize flag and is only exchanged at TCP connection establishment. The urgent flag.

Applicable to:

NS-series Sensors

set auditlog

Configure the Sensor to begin or stop archival of audit logs.

Syntax:

```
set auditlog <enable | disable>
```

where: `<enable>` allows the audit log feature to record system events

`<disable>` stops the audit log feature from recording system events

Default Value:

enable

Example:

```
set auditlog enable
```

Applicable to:

NS-series Sensors

set fips sharedkey

This command is used to authenticate the Primary and the Secondary Sensors in FIPS mode. The Primary and the Secondary Sensors exchange the symmetric key (user configured keys) for authentication. Any difference in key specifications will result in authentication failure.

The symmetric key can be created only in FIPS mode.

Syntax:

```
set fips sharedkey
```

The symmetric key must be entered once from the Primary Sensor and once from the Secondary Sensor.

Applicable to:

NS9300 Sensors

set password age

Allows you to set a limit on password validity period.

Syntax

```
set password age <days>
```

Where days can be between 10-99 days.

Applicable to:

NS-series Sensors

set password length

Allows you to set the length of the password

Syntax

```
set password length <number of characters>
```

Where number of characters can be between 15-255.

Applicable to:

NS-series Sensors

set sensor sharedsecretkey

Sets the shared secret key value that the Manager and Sensor use to establish trust.

Type the command as shown in the syntax below. The Sensor prompts you for a secret key value. The value you enter is not shown. You will be prompted to type the value a second time to verify that the two entries match.

The **sharedsecretkey** value you enter in the CLI to identify the Sensor must match the Manager interface shared secret key. If the shared secret keys between the Manager interface and Sensor CLI do not match, then the Manager and Sensor cannot communicate. If you want to change the shared secret key, you must change the value in the CLI as well as the Manager interface.

Syntax:

```
set sensor sharedsecretkey
```

At the Sensor's prompt for a secret key value, enter a case-sensitive character string between 8 and 25 characters of any ASCII text. The shared secret key value is case sensitive. For example, IPSkey123.

Sample Output:

On executing the command, the following messages are displayed

- When the Sensor is installed:

  ```
  sensor is already installed, please do a deinstall before changing this parameter
  ```

- When Sensor is deinstalled:
  - ```
    intruShell@john> set sensor shared secretkey
    Please enter shared secret key:

    Please Re-enter shared secret key:

    This will take a couple of seconds, please check status on CLI
    ```
  - ```
    ntbaSensor@vNTBA> set sensor sharedsecretkey
    Please enter shared secret key:

    Please Re-enter shared secret key:

    This will take a couple of seconds, please check status on CLI
    ```

If the Sensor and Manager already has a CA-signed certificate chain, then it will try to establish trust with the Manager using the CA-signed certificate chain. If CA-signed certificate does not exist in the Manager does, then the Sensor reverts to the self-signed certificate chain.

Applicable to:

NS-series Sensors

set sshlog

Use this command to enable or disable SSH logging (archiving SSH activity into log files).

Syntax

```
set sshlog <enable/disable>
```

It is disabled by default.

Applicable to:

NS-series Sensors

show

Shows all the current configuration settings on the Sensor like model, installed software version, IP address, and Manager details.

This command has no parameters.

Syntax:

```
show
```

Information displayed by the `show` command includes:

[Sensor Info]

- System Name
- Date
- System Uptime
- System Type
- System serial number (displays the primary, secondary and master/system serial numbers separately in case of NS9300)
- Software Version
- Hardware Version
- MGMT Ethernet Port
- MGMT port Link Status

[Sensor Network Config]

- IP Address
- Netmask
- Default Gateway
- SSH Remote Logins

[Manager Config]

Self Signed cert support

- Install TCP Port
- Alert TCP Port
- Logging TCP Port

CA Signed cert support

- Install TCP Port
- Alert TCP Port
- Logging TCP Port
- FIPS Mode
- Admin SSH/Console Access

Sample Output:

For Sensor, the output is as shown:

```
intruShell@john> show

[Sensor Info]

System Name : NS9300

Date : 7/12/2018 - 9:14:9 UTC

System Uptime : 03 hrs 15 min 35 secs
```

```
System Type : IPS-NS9300

Serial Number : J021834009

Software Version : 9.1.166.26

Hardware Version : 1.30

MGMT Ethernet port : auto negotiated

MGMT port Link Status : link up

[Sensor Network Config]

IP Address : 10.213.174.202

Netmask : 255.255.255.0

Default Gateway : 10.213.174.201

SSH Remote Logins : enabled

[Manager Config]

Self Signed cert support

Install TCP Port : 8501

Alert TCP Port : 8502

Logging TCP Port : 8503

CA Signed cert support

Install TCP Port : 8506

Alert TCP Port : 8507

Logging TCP Port : 8508
```

Applicable to:

NS-series Sensors

show fips mode status

Displays the status of the FIPS mode.

Syntax

```
show fips mode status
```

This command displays the following information:

- FIPS mode status - Displays the status as enabled
- The admin SSH/console access status

Applicable to:

NS-series Sensors

show firmware version

Shows the current bootloader version information running on the Sensor.

Syntax

```
show firmware version
```

Above command is available in debug mode. Type `debug` to log on to debug mode. Once in debug mode, type `disable` to get out of debug mode.

Applicable to:

NS-series Sensors

show ssh config

Displays the SSH version, client configuration, and sever configuration information.

Syntax:

```
show ssh config
```

Sample output:

```
SSH Version: OpenSSH_7.6p1, OpenSSL 1.0.2m-fips 2 Nov 2017

SSH Client Configuration :

Ciphers : aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes128-ctr

MACs : hmac-sha2-256,hmac-sha2-512,hmac-sha1

KexAlgorithms : ecdh-sha2-nistp256,diffie-hellman-group14-sha1

SSH Server Configuration :

Ciphers : aes256-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com

MACs : hmac-sha1,hmac-sha2-256,hmac-sha2-512

KexAlgorithms : diffie-hellman-group14-sha1

PublickeyAuthentication : Enabled

PasswordAuthentication : Enabled
```

Applicable to:

NS-series Sensors

status

Shows Sensor system status, such as System Health, Manager communication, signature set details, total number of alerts detected, and total number of alerts sent to the Manager.

This command has no parameters.

Syntax:

```
status
```

Sample Output:

For Sensor, the output is as shown:

```
[Sensor]

System Initialized : yes
```

```
System Health Status : good
Layer 2 Status : normal (IDS/IPS)
Installation Status : opening channel in progress
IPv6 Status : Dont Parse and Allow Inline
Reboot Status : Not Required
Guest Portal Status : up
Hitless Reboot : Available
Last Reboot reason : resetconfig issued from CLI
[Signature Status]
Present : yes
Version : 9.8.20.2
Geo Location database : Present
DAT file : Present
DAT file Version : 2047.0
[Manager Communications]
Trust Established : no
Alert Channel : down
Log Channel : down
Authentication Channel : down
Last Error : Alert Channel - unknown: 13
Alerts Sent : 0
Logs Sent : 0
[Alerts Detected]
Signature : 0 Alerts Suppressed : 0
Scan : 0 Denial of Service : 0
Malware : 0
[McAfee MATD Communication]
Status : down
IP : 0.0.0.0
Port(Secure) : 8505
FIPS Mode : Enabled
```

```
Admin SSH/Console Access: Enabled
```

If there is a failure in establishing trust relationship between the Sensor and Manager due to mismatch in shared secret key, the `Last Error` displays the message `Alert Channel - Install Keys Mismatch`. In such an instance, check the shared secret key on the Manager and set it on the Sensor using `set sensor sharedsecretkey` command.

Applicable to:

NS-series Sensors

traceupload

Uploads an encoded diagnostic trace file to the configured SCP server from which you can send it to McAfee Technical Support for diagnosing a problem with the Sensor. A trace upload facility is also available in the Manager interface.

Syntax:

```
traceupload scp WORD
```

where `WORD` stands for the file name to which the trace must be written.

For NS-series Sensors, when loading an encoded diagnostic trace file to the SCP server, the first attempt will be based on SSH public key authentication if that fails the Sensor will fall back to the password authentication. If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

As part of traceupload, additional information is collected using logstat. Due to this, additional time is required to collect logs from the Sensor, and can take around 10-30 minutes based on the Sensor model.

Applicable to:

NS-series Sensors

4 Manager user interfaces for Certification

For information about all other Manager user interfaces, refer to the *McAfee Network Security Platform 10.1.x Product Guide*.

Contents

SSH public key based authentication for Manager Appliance (Linux)

You can use SSH public key authentication or password based authentication to login to the Manager or the remote machine using SSH. Use of public key authentication allows administrators and users to access the Manager or the remote machine without the use of password based authentication.

Manager as the SSH client

When the Manager serves as the SSH client, you can SCP files to a remote machine serving as a SCP server from the Manager. This requires the SSH public key generated on the Manager to be configured on the remote SCP server. The Manager uploads the key to the remote SCP sever. Perform the following steps to access the SCP server on a remote machine from the Manager:

1. Login to the Manager appliance with the username and password.
2. Execute the command `publicKeyAuth`.
3. Choose `Upload Key To A Server` and press enter.
4. Enter the SCP server IP address.
5. Enter the SCP server username.
6. Enter the SCP server password to transfer the public key to the remote machine.
   The public key is successfully uploaded to the remote machine.
7. To check if the key is uploaded, try logging into the machine, with `ssh <username>@<SCP server IP address>`.
   The SSH public key based authentication is successful.

Sample output

```
MLOS-78> publicKeyAuth

Choose one of the below options

1: Upload Key To A Server

2: Download Key From Client
```

```
Input [1] or [2] : 1

[sudo] password for admin:

Please provide with the following inputs.

[Thu Feb 20 10:57:44 UTC 2020] : Enter The SCP Server IP : 10.1.1.1

[Thu Feb 20 10:57:44 UTC 2020] : Enter SCP Server UserName : admin

[Thu Feb 20 10:57:44 UTC 2020] : Checking if .ssh/ already exists.

[Thu Feb 20 10:57:44 UTC 2020] : The /home/admin/.ssh already exists!

[Thu Feb 20 10:57:44 UTC 2020] : Checking if public key already exists.

[Thu Feb 20 10:57:44 UTC 2020] : The /home/admin/.ssh/id_ecdsa.pub does not exists!

[Thu Feb 20 10:57:44 UTC 2020] : Creating a key pair.

Generating public/private ecdsa key pair.

Your identification has been saved in /home/admin/.ssh/id_ecdsa.

Your public key has been saved in /home/admin/.ssh/id_ecdsa.pub.

The key fingerprint is:

SHA256:7M1msETM8MRYZGqNnRDx+OV/anEOCQfxcbAUe2q+Dno admin@MLOS-78

The key's randomart image is:

+---[ECDSA 256]---+

| +B+ ..=o.|

| oXo..o = |

|=*= ..+ .|

|. .=+. .o |

|.o So...|

| .o. .+o. |

|..o. .=+ .|

|. o..+E+ |

| o..o. .|

+----[SHA256]-----+

[Thu Feb 20 10:57:44 UTC 2020] : Successfully created the key pair.

[Thu Feb 20 10:57:44 UTC 2020] : Changing permissions of local .ssh/ dir

[Thu Feb 20 10:57:44 UTC 2020] : Successfully changed the permissions of the dir/file
to 700

[Thu Feb 20 10:57:44 UTC 2020] : Transfering public key to remote machine. The
operation might ask for password.
```

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/
id_ecdsa.pub"

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
any that are already installed

/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now
it is to install the new keys

FIPS mode initialized

admin@10.1.1.1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'admin@10.1.1.1'"

and check to make sure that only the key(s) you wanted were added.

[Thu Feb 20 10:57:44 UTC 2020] : Successfully copied the key to 10.1.1.1

[Thu Feb 20 10:57:44 UTC 2020] : Modifying .ssh/ related dir/file permissions on the
remote machine. The operation might ask for password.

FIPS mode initialized

[Thu Feb 20 10:57:44 UTC 2020] : Successfully modified the permissions of .ssh/
authorized_keys on remote machine.
```

Manager as the SSH server

When the Manager serves as the SSH server, you can SCP files from a remote machine serving as a SCP client to the Manager. This requires the SSH public key generated on the remote SCP client to be configured on the Manager. The Manager downloads the key from the remote SCP client. Perform the following steps to access the Manager from the SCP client on a remote machine:

1. Login to the Manager appliance with the username and password.
2. Execute the command `publicKeyAuth`.
3. Choose `Download Key From Client`.
4. Enter the SCP client IP address.
5. Enter the SCP client username.
6. Enter the public key file location given on the SCP client machine.
7. Enter the SCP client password to transfer the public key to the remote machine.

   The public key is successfully downloaded from the remote machine. The SSH public key based authentication is successful.

Sample output

```
MLOS-78> publicKeyAuth

Choose one of the below options

1: Upload Key To A Server

2: Download Key From Client

Input [1] or [2] : 2
```

```
[sudo] password for admin:

Please provide with the following inputs.

[Thu Feb 20 10:51:14 UTC 2020] : Enter The SCP Client IP : 10.1.1.1

[Thu Feb 20 10:51:14 UTC 2020] : Enter SCP Client UserName : admin

[NOTE] : Please Make Sure The Public Key Is Generated Using ECDSA

[Thu Feb 20 10:51:14 UTC 2020] : Public Key File Location On Client : /home/
admin/.ssh/id_ecdsa.pub

[Thu Feb 20 10:51:14 UTC 2020] : The /home/admin/.ssh already exists!

[Thu Feb 20 10:51:14 UTC 2020] : Changing permissions of local .ssh/ dir

[Thu Feb 20 10:51:14 UTC 2020] : Successfully changed the permissions of the dir/file
to 700

[Thu Feb 20 10:51:14 UTC 2020] : Downloading Public Key from Client : 10.1.1.1 to
Server

FIPS mode initialized

admin@10.1.1.1's password:

id_ecdsa.pub 100% 177 326.2KB/s 00:00

[Thu Feb 20 10:51:14 UTC 2020] : Validating Public Key Algorithm

Download Successful

[Thu Feb 20 10:51:14 UTC 2020] : Resetting the permissions of the file .ssh/
authorized_keys on local machine

[Thu Feb 20 10:51:14 UTC 2020] : Successfully modified the permissions of .ssh/
authorized_keys on remote machine.
```

FIPS-related Manager user interfaces

You should update the **ems.properties** file for various settings explained in the sections below. This file is available at `/opt/NetworkSecurityManager/App/config/`.

View Details

Go to **Devices** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Summary**.

The details includes a field called **FIPS Mode** that displays FIPS compliance information for an installed Sensor. The **FIPS Mode** field displays whether FIPS is enabled, disabled or not supported in the Sensor.

TACACS+ authentication

Go to **Devices** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Setup** | **Remote Access** | **TACACS+**.

When FIPS mode is enabled in the Sensor, configuration for TACACS+ authentication is disabled.

Packet Log Encryption

Go to **Devices** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Setup** | **Advanced** | **Alerting Options**.

When FIPS mode is enabled in the Sensor, packet log channel encryption cannot be enabled or disabled. By default, **Enable Packet Log Channel Encryption** will be checked (enabled) and grayed out in **Response Action Settings** page.

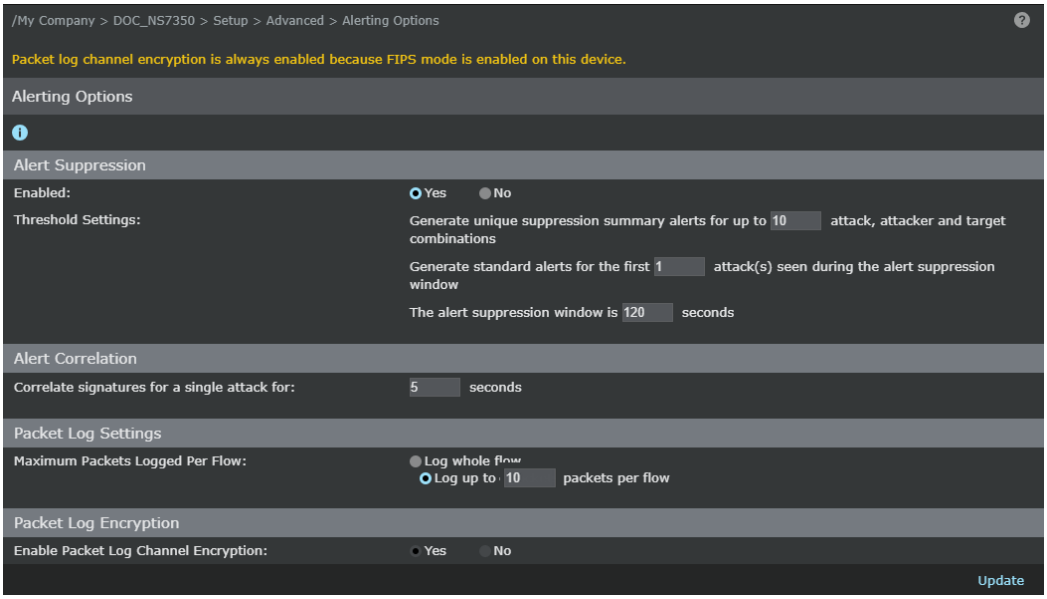

Figure 4-1 Sensor action settings page

Importing a Sensor's configuration

Go to **Devices** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Maintenance** | **Import Configuration**.

While importing a Sensor configuration file from a non-FIPS-enabled Sensor to a FIPS-enabled Sensor, the configurations that are not supported in the FIPS mode are ignored.

Sensor Failover

Go to **Devices** | **<Admin Domain Name>** | **Global** | **Failover Pairs**.

When one of the Sensors in a failover pair is FIPS-enabled, it is required that the peer Sensor is also FIPS-enabled.

Sensor Report

Go to **Manager** | **<Admin Domain Name>** | **Reporting** | **Configuration Reports** | **IPS Sensor**.

The Sensor report displays the **FIPS Mode** field with the status of the configuration. The Sensor Information table displays whether the FIPS mode is enabled, disabled, or not supported in the Sensor.

Certificate Expiration Fault

To view the fault information, select **Manager** | **<Admin Domain Name>** | **Troubleshooting** | **Logs** | **Faults**.

The Manager raises a fault if a certificate has either expired or is approaching expiration. This check is done as part of scheduled file pruning and will not be done during Manager start-up.

Logon History

This feature is enabled by setting this property in **ems.properties**:

```
iv.access.control.authentication.loginHistoryTimePeriodLastNumberOfDays=30
```

To view **Recent Logon History** window, click **Login History** link in the header bar located on top of the menu bar.

The **Recent Logon History** window displays failed and successful logon attempts for a number of days set in **ems.properties**.

The period of time is set by assigning a value to the `loginHistoryTimePeriodLastNumberOfDays` property in the **ems.properties** file. If this property is not defined or set to -1 in the **ems.properties** file, then the **Recent Logon History** page will display failed logon attempts.

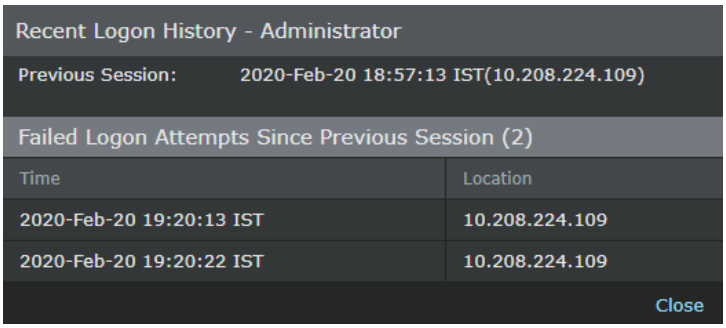

Figure 4-2 Logon history

Shutdown on audit failure

This feature is enabled by setting this property in **ems.properties**:

```
iv.core.audit.ShutDownOnAuditFailureEnabled=true
```

The Manager must invoke a system shutdown in the event of an audit failure. If the audit system detects an exception while attempting to audit to database, or audit to file then it shuts down the Manager. Note that since audit failure forcibly shuts down the Manager, it requires the Manager to be manually restarted. Server logs contain the root cause of audit failure. Also, system fault is listed after the Manager is successfully restarted.

5 Handling user password between FIPS and non-FIPS images

The MD5/SHA1 algorithm standards are used by non-FIPS sensor images to verify a user password. FIPS capable Sensor images use the SHA-512 algorithm standard to verify the user password.

FIPS images require passwords to satisfy the following criterion.

- Password length should be of minimum 15 characters.
- Password should at the least contain 2 lower case, 2 upper case letters, 2 numeric and 2 special characters.
- Must differ from the previous password by atleast 4 characters
- Must not be reused from the last 10 passwords
- Password expire in 45 days

There can be issues during upgrade or downgrade between FIPS and non-FIPS Sensor images as mentioned below:

- **The default admin password has not changed:** If there is no change in the default password, no conflict arises during upgrade/downgrade.
- **The default admin password has changed with non-FIPS capable image:** If there is a change in the FIPS capable image, the password is reset to default.The initial bootup script of the FIPS capable image detects the password format to be of MD5 format and deletes it. The password is then reset to default SHA-256 supported format.
- **The default admin password has changed with FIPS capable image:** Any change to a non-FIPS capable image, will result in the password being reset to default. This process of resetting the password is done when the image is downloaded. The newly downloaded image version is compared to a tag, and if the newly downloaded image is non-FIPS capable, the image is deleted. The password is then reset to default MD5 supported format.

Upgrade or downgrade from non-FIPS to FIPS images

On a transition from non-FIPS to FIPS image, you can only login with default admin password. Since this default admin password is not FIPS compliant, you will be prompted to change the default admin password.

If you had previously changed your password in a non-FIPS image, logging into the FIPS Sensor requires the default admin password for a FIPS images. The automatic configuration reset enforces the FIPS default password. The Manager notifies about this reset.

Upgrade or downgrade from FIPS images to non-FIPS

A transition from FIPS to non-FIPS will result in password being reset to default. You can only login using the default passwords for admin of the non FIPS image.

A Appendix: Network Security Platform Documentation List

To find Network Security Platform product documentation:

Task

1 Go to McAfee Documentation Portal (https://docs.mcafee.com/).

2 Scroll to the **Products A-Z** section in the landing page.

3 Click **Network Security Platform/Virtual Network Security Platform**.

The **Network Security Platform/Virtual Network Security Platform** documentation list is displayed.

4 To view documentation for a particular version, use the **Product** filter in the left pane.

Software Documentation
Installation Guide
Product Guide
Integration Guide
Manager API Reference Guide

Table A-1 Network Security Platform hardware documentation

Guide	Models
Manager Appliance Product Guide	McAfee Linux Operating System (MLOS)
NS-series Sensor Product Guide	NS9500, NS9x00, NS7x50, NS7x00, NS5x00, NS3500, and NS3x00

Table A-1 Network Security Platform hardware documentation *(continued)*

Guide	Models
NS-series Reference Guide	**1** NS-series Interface Modules **2** NS-series Transceiver Modules **3** NS-series Sensors DC Power Supply Installation
Fail-Open Kit Product Guide	• 100 Gigabit Modular Active Fail-Open Bypass Kit • 40 Gigabit Modular Active Fail-Open Bypass Kit • 1/10 Gigabit Modular Active Fail-Open Kit • 1/10 Gigabit Modular Passive Fail-Open Kit • 40 Gigabit Active Fail-Open Bypass Kit Guide • 10/100/1000 Copper Active Fail-Open Bypass Kit with SNMP • 10/100/1000 Copper Active Fail-Open Bypass Kit • 1 Gigabit Optical Active Fail-Open Bypass Kit • 10 Gigabit Optical Active Fail-Open Kit • 10/100/1000 Copper Passive Fail-Open Kit • 1 Gigabit Optical Passive Fail-Open Bypass Kit • 10 Gigabit Optical Passive Fail-Open Kit

B Appendix: Audit Log Records

This section describes the audit log records in relation to a user's activities. The general format of audit records is:

```
Timestamp, Appliance Name, Process/Function, Message
```

An example of an audit record is:

```
NSMAppliance sshd[3694]: Disconnecting: Too many authentication failures [preauth]
```

When displayed in the GUI, this information is further broken out into:

```
Date, Admin Domain, User, Attack Category, Action, Result, Description
```

An example of an audit record displayed in the GUI is:

Date	Admin Domain	User	Attack Category	Action	Result	Description	Commit Comments	Audit Data Details
2020-02-20 19:20:06 IST	/My Company	Administrator	User	Manager Console Logout	Success	User "Administrator" with login id "admin" logged out of the Manager from "10.208.224.109 (10.208.224.109)".		

The following table documents the messages within audit log records generated by McAfee Network Security Platform.

Table B-1 Audit Log Records

Action	Log Message
Changes to the system time by an Administrator	Time has been changed
Communication between the Manager and Sensors	• **Enabling**: Successfully added sensor "*sensor_name*" • **Disabling**: Successfully deleted sensor "*sensor_name*"
Failure to establish a TLS Session	• Certificate having missing Extended keys • Mismatch between configured Server Name and Subject Alt Name in Imported certificate • The connection to syslog server *IP_Address:port_number* failed. Error: Syslog TCP connection failed.
Failure to establish an HTTPS Session	Mismatch between configured Server Name and Subject Alt Name in Imported certificate
Failure to establish an SSH session	• Disconnecting: Too many authentication failures [preauth] • Unable to negotiate with *IP_Address* port *port_number*: no matching host key type found. Their offer: *host_key_type* [preauth] • Unable to negotiate with *IP_Address* port *port_number*: no matching key exchange method found. Their offer: *key_exchange_method* [preauth]

Table B-1 Audit Log Records *(continued)*

Action	Log Message
Management activities of system data	• Read audit log • Successfully set Session Timeout • Logon Banner Configuration updated • Successfully set Password Content, Configuration is ...

Trusted connections	• **Initiation**:
	  • Pktlog Channel back up. Clear the Pktlog Channel Down event of sensor *sensor*
	  • Alert Channel back up. Clear the Alert Channel Down event of sensor *sensor*
	  • Syslog Client - Added to Retry Q
	  • Syslog Client - Flushing and Shutting down
	  • Request for Authentication for User name=*Username*
	• **Termination**:
	  • The link on Port: *Port_identifier* is Down Count: *number*. The link between this port and the external device to which it is connected is down.
	  • Received disconnect from *IP_Address* port *port_number*: disconnected by user
	  • User "*User Name*" with login id "*Username*" logged off Network Security Manager from "*Hostname* (*IP_Address*)"
	• **Failure**:
	  • Certificate having missing Extended keys
	  • Mismatch between configured Server Name and Subject Alt Name in Imported certificate
	  • Received fatal alert: handshake_failure
	  • Connection refused (Connection refused)
	  • Disconnecting: Too many authentication failures [preauth]
	  • Unable to negotiate with IP_Address port *port_number*: no matching host key type found. Their offer: *hostkey_type* [preauth]
	  • Unable to negotiate with *IP_Address* port *port_number*: no matching key exchange method found. Their offer: *key_exchange_method* [preauth]

Unsuccessful attempt to validate an X.509 certificate	• Certificate having missing Extended keys • Mismatch between configured Server Name and Subject Alt Name in Imported certificate
Unsuccessful login attempts limit is met or exceeded	Login failed: Maximum allowable login attempts *number* have exceeded

Table B-1 Audit Log Records *(continued)*

Action	Log Message
Use of the identification and authentication mechanism	• Postponed keyboard-interactive/pam for *username* from *IP_Address* port *port_number* ssh2 [preauth] • Postponed publickey for *username* from *IP_Address* port *port_number* ssh2 [preauth] • Accepted keyboard-interactive/pam for *username* from *IP_Address* port *port_number* ssh2 • error: Could not load host key: *path_to_hostkey_file* • Failed keyboard-interactive/pam for *username* from *IP_Address* port *port_number* ssh2 • Failed publickey for *username* from *IP_Address* port *port_number* ssh2: RSA SHA256:*public_key_value* • User "*username*" failed to log in to Network Security Manager from "*Hostname* (*IP_Address*)". Login URI: /intruvert/jsp/module/Login.jsp. URI referrer : https://*Hostname*//intruvert/jsp/module/Login.jsp , protocol : HTTP/1.2 • Unknown login ID "*Username*". Login failed from "*Hostname* (*IP_Address*)". Login URI: /intruvert/jsp/module/Login.jsp. URI referrer : https://*Hostname*//intruvert/jsp/module/Login.jsp , protocol : HTTP/1.2 • Starting Session *number* of user *Username* • Network Security Manager Login failed at *timestamp*
User session terminated	• · Removed session *number*. • User "*User Name*" with login id "*Username*" logged out of the Manager from "*Hostname* (*IP_Address*)". • Close session: user *Username* from *IP_Address* port *port_number* id *number*

Index