Configure NTP Authentication on Secure Network Analytics

Contents

Introduction

This document describes how to configure your Secure Network Analytics (SNA) appliance to authenticate the connection to the configured NTP Server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Network Analytics appliance administration
- Network time protocol (NTP)

Components Used

The Cisco Secure Network Analytics Manager appliance used for this document is version 7.4.2.

This process applies to all Cisco Secure Network Analytics appliance types.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

NTP configuration requirements

The values used for authenticating the NTP communication must meet these requirements:

- The Key ID value must be less than or equal to 65535
- The Key validation is SHA1
- The Key Value must be no longer than 32 printable alphanumeric characters (ASCII): 0-9, A-Z, a-z, and symbols (except #)

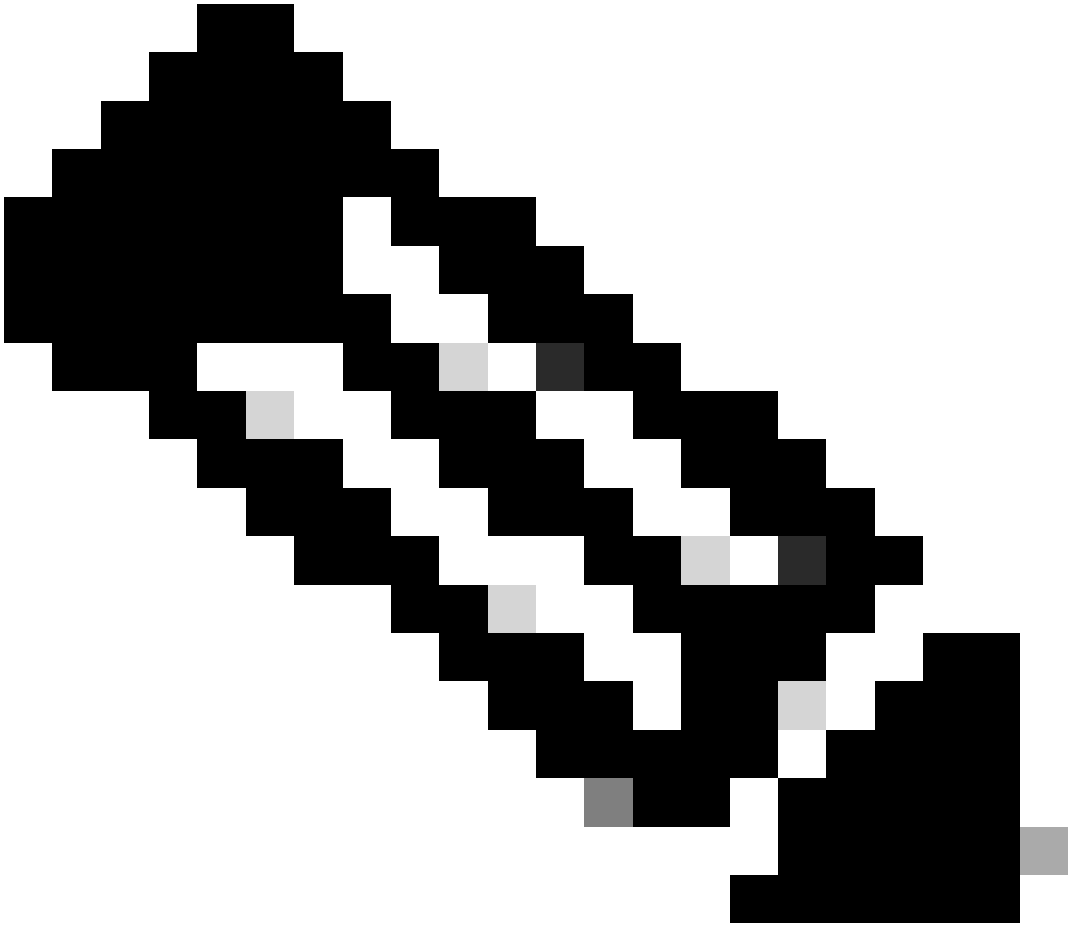
Key Value details

NTP assumes that Key Values longer than 20 bytes are assumed to be HEX.

The maximum length of the Key Value is 64 bytes so a de-hexed key can be no longer than 32 bytes.

Refer to the table for example key values for the NTP server and Secure Network Analytics appliance.

Key byte	NTP Server Key Value Configuration	Secure Network Analyt Configuration
Less than 20 bytes	Lan1cope!	Lan1cope!
Between 20 bytes and 32 bytes	4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163	Lan1cope!Lan1cope!La



Note: The values used in the table are examples only and not a recommended value to be used in your environment

Configuration SNA Manager NTP Authentication

Open NTP Server settings

Login to the **SNA Manager** , and open **NTP Server** settings.

1. From the main menu, select Configure > GLOBAL Central Management.
2. From the Inventory tab, click the ... **(**Ellipsis **)** icon for the appliance.
3. Select Edit Appliance Configuration.
4. Select the Network Services tab.

Add an NTP Server

Use these instructions to add an NTP server to the selected appliance configuration if needed.

1. In the NTP Server section, click Add New.

2. In the NTP Servers field, click the drop-down arrow. Select an NTP server from the list.
3. Enter the server name or IP address.
4. Click Add.
5. Click Apply Settings.
6. Accept the on-screen prompts. The appliance reboots automatically.

Add Authentication

Use these instructions to authenticate the connection to the selected NTP server.

Preparation: Make sure you have the NTP server key ID and key value.

1. In the NTP Server section, click the ... **(**Ellipsis**)** icon for the NTP server.
2. Select Authenticate Connection.
3. Enter the key ID and key value.
4. Click Apply Authentication.
5. Click Apply Settings.
6. Accept the on-screen prompts. The appliance reboots automatically.

Verify

Confirm Authentication

If you add authentication to a server, the key icon indicates authentication is configured. Make sure you review the audit log to confirm the authentication is successful.

1. From the main menu, select Configure > GLOBAL Central Management.
2. From the Inventory tab, click the ... **(**Ellipsis **)** icon for the appliance.
3. Select Support.
4. Select the Audit Logs tab.
5. In the Category field, select Management.
6. Click Search.
7. Confirm the NTP communication status and system time changes are shown as successful. (Check the Success column to confirm the event is shown as Yes).

Troubleshoot

Confirm byte count

You can use a shell on a Linux device to test the byte count of the Key Values.

The Key Values in the examples come from the table in the Key Value Length section in this document.

Run the `echo -n '{key_value}' | wc -c` command to see the byte count replacing {key_value} with the key value you wish to use.

```
742smc:~# echo -n 'Lan1cope!' | wc -c
9
742smc:~# echo -n 'Lan1cope!Lan1cope!Lan1cope!Lan1c' | wc -c
32
742smc:~# echo -n '4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163' | wc -c
64
```

```
742smc:~#
```

The output on lines 2, 4, and 6 show that the key value byte counts are 9, 32, and 64 respectively.

Confirm Character Usage

If the byte count is less than 20, ensure you are using ASCII printable characters as noted in the NTP configuration requirements.

You can run the echo '{key_value}' | xxd -r -p && echo command to convert the HEX values in to ASCII replacing {key_value} with the key value you wish to use.

```
742smc:~# echo '4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163' | xxd -r -p && echo
Lan1cope!Lan1cope!Lan1cope!Lan1c
742smc:~#
```