Generate Diagnostics Pack for Secure Network Analytics Appliances

Contents

Introduction

Procedure

- Method 1. Via SystemConfig Menu (Recommended Method)
- Method 2. Central Management
- Method 3. Admin Web UI
- Method 4. From Each Appliances Command Line Interface (CLI)

Generating a CXD Upload Token

- Using the upload token from within SystemConfig
- Use the upload token from within the SNA Web UI (new to 7.6.1)

Troubleshoot

Related Information

Introduction

This document describes the different procedures available to generate a Diagnostics Pack for Secure Network Analytics (SNA) Appliances.

Procedure

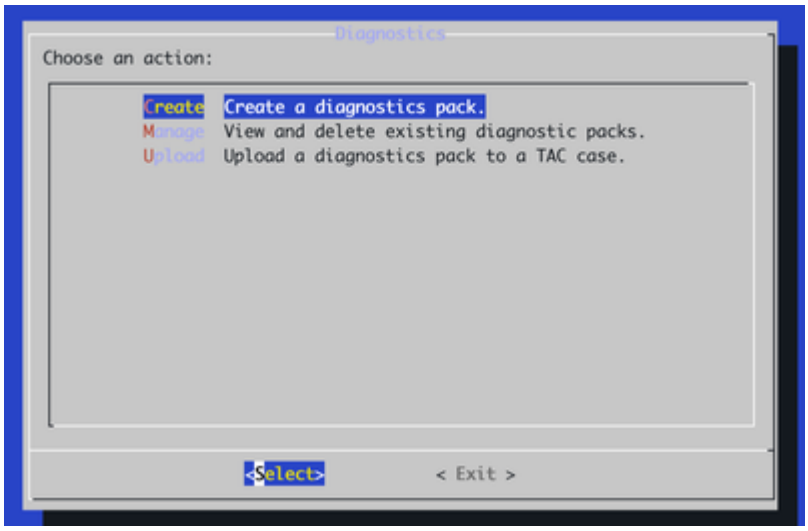
There are four methods to generate the Diagnostics Pack for the SNA appliances. The recommended method is **Method 1. Via SystemConfig Menu**.

The remaining methods are an option in case your appliance does not have Internet connectivity directly or via proxy.

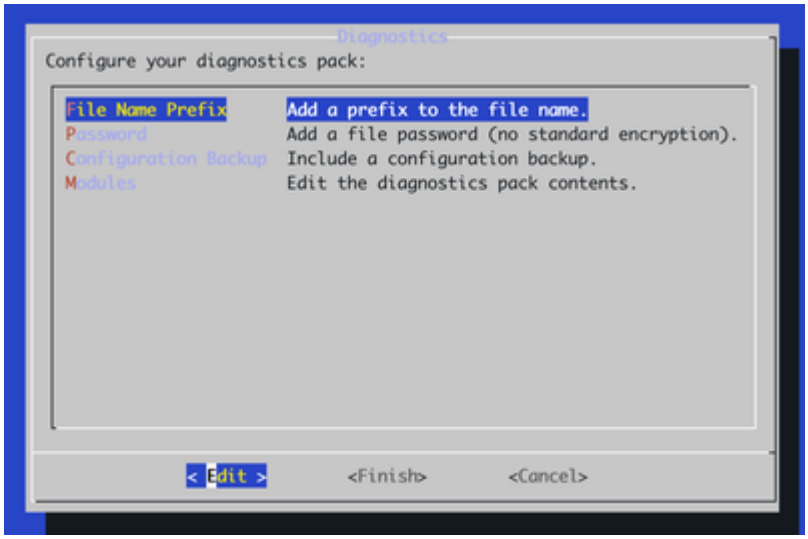
Available methods vary based on the software release.

Method 1. Via SystemConfig Menu (Recommended Method)

1. Log in to the appliance console as sysadmin.
2. Select **Recovery > Diagnostics Pack > Create**.



3. To customize your diagnostics pack, highlight a desired option and then click **Edit**.



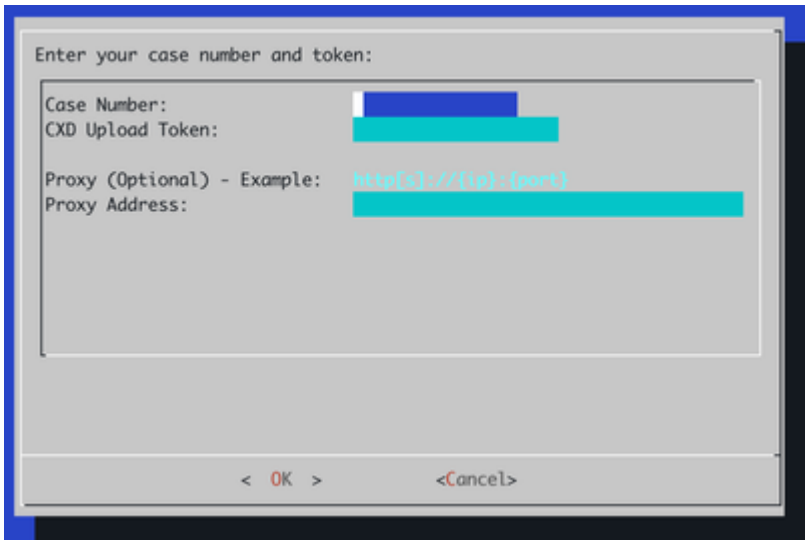
Options:

File Name Prefix - Add a file name prefix for your diagnostics pack (maximum of 127 characters).
Password - Create a file password for your diagnostics pack. If you do not create a file password, the diagnostics pack is encrypted with the default method (Cisco key).
Configuration Backup - Select this option and complete the onscreen prompts to include a configuration backup in your diagnostics pack. For more information about backups, refer to Backup Configuration Files in the Help.
Modules - Edit the diagnostic pack contents by selecting the specific modules you want to include.

4. Click **Finish**. Complete the on-screen prompts to create the diagnostics pack.

5. You are able to upload the Diagnostic Pack directly to your TAC case from SystemConfig. Select **Upload.**

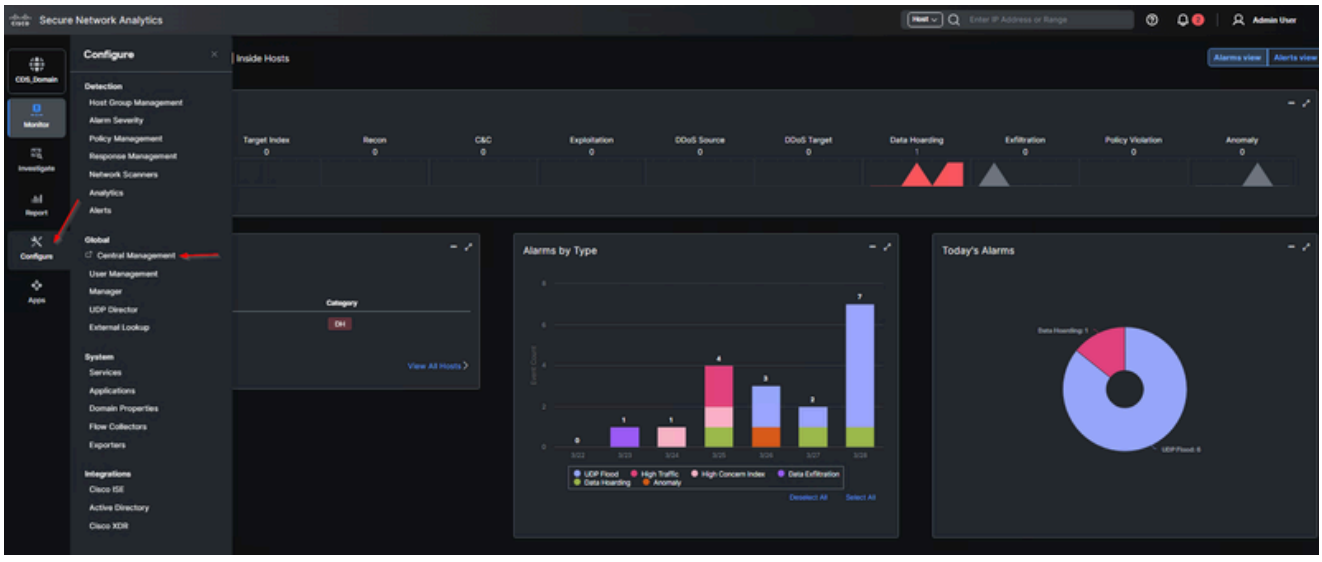
6. Select the Diagnostic Pack you wish to upload and select **Select**.



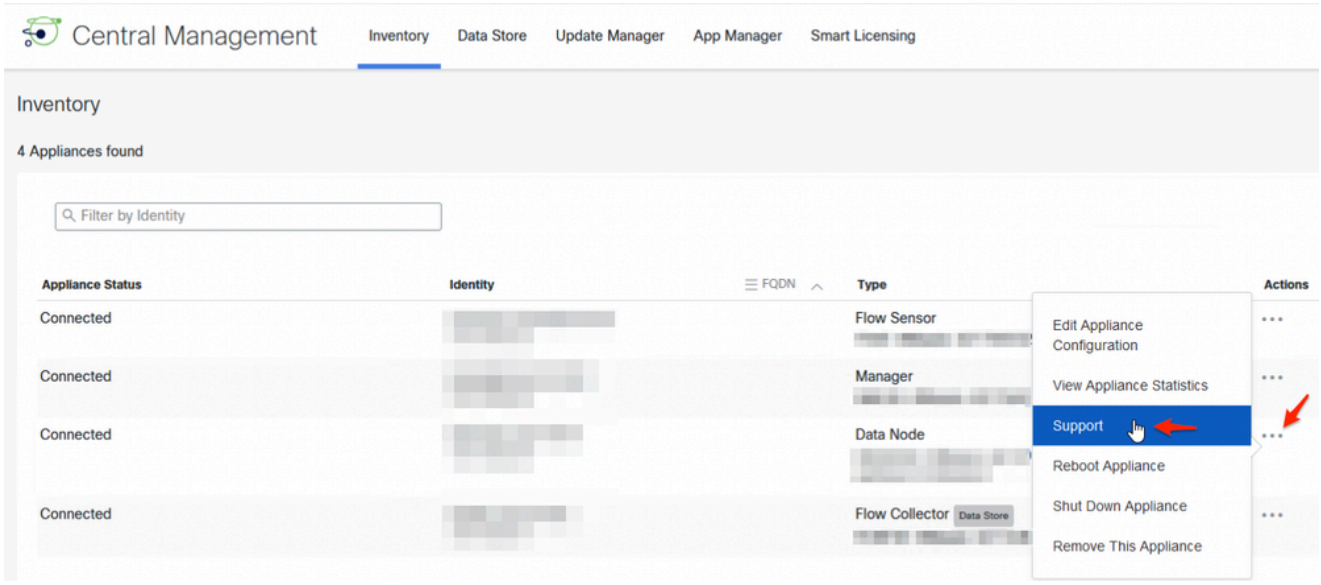
7. Enter the TAC Case Number in the **Case Number** field.
8. Enter the Case number token **CXD Upload Token** field. If you do not have this token, generate one using the steps here: https://www.cisco.com/c/en/us/support/web/tac/tac-customer-file-uploads.html#cxduploadtoken
9. If a proxy is needed, enter it in the **Proxy Address** field.
10. Select **OK** when complete.

Method 2. Central Management

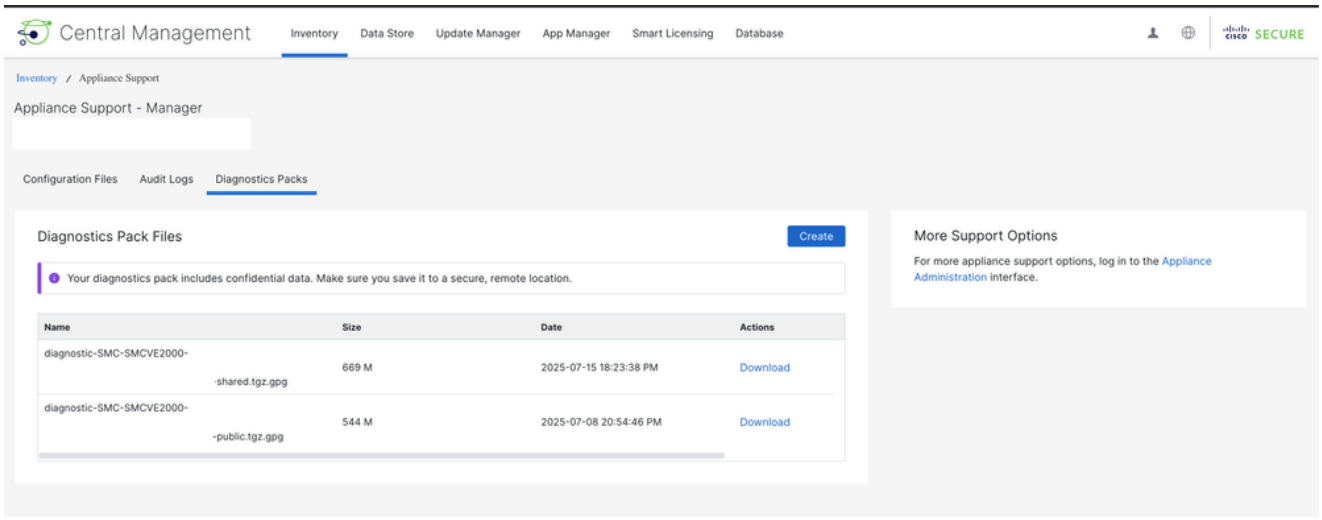
1. Log in to the Web UI of the SNA Manager.
2. Select **Configure > Global > Central Management**



3. A browser tab opens for Central Management and shows the Inventory tab. From the Inventory tab, click the ellipsis icon for the appliance you wish to create a diagnostic pack for. Select Support.



4. This takes you to that appliances support page within Central Management. Click "Diagnostics Packs" tab > Create to start the process of creating a new diagnostic pack. Previously completed Diagnostic Packs can be downloaded.

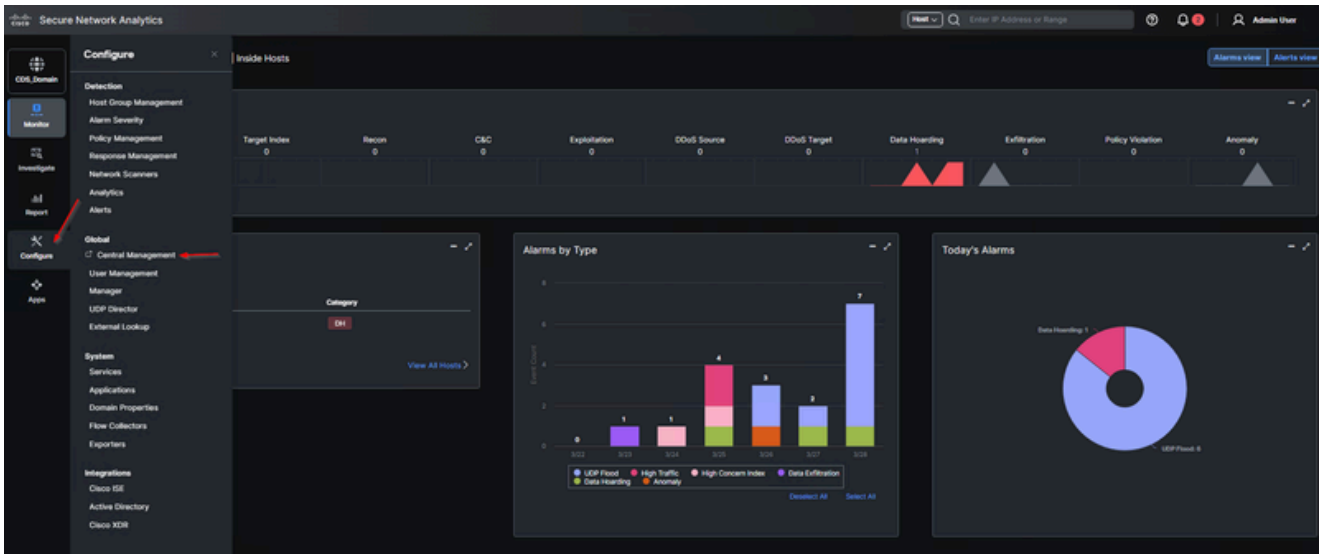


Method 3. Admin Web UI

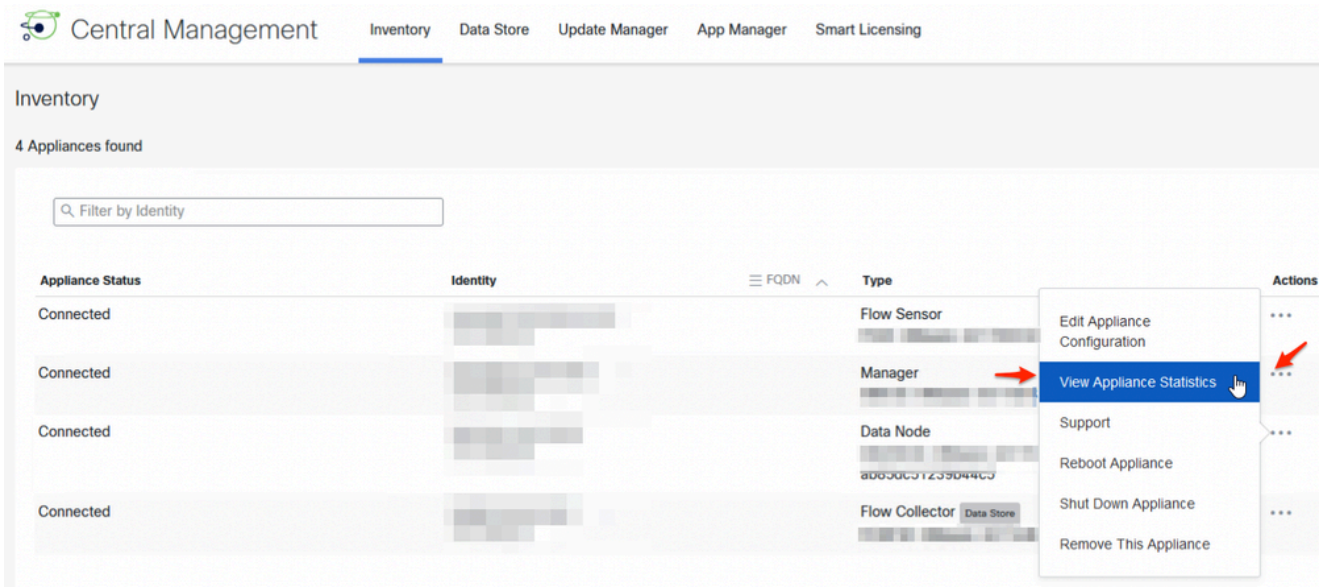
The are two methods of accessing the Admin UI of an SNA appliance, either through the SNA Managers Central Management feature, or directly.

If you know your appliances FQDN or IP Address, start at step 4.

1. Log in to the Web UI of the SNA Manager.
2. Select **Configure > Global > Central Management**



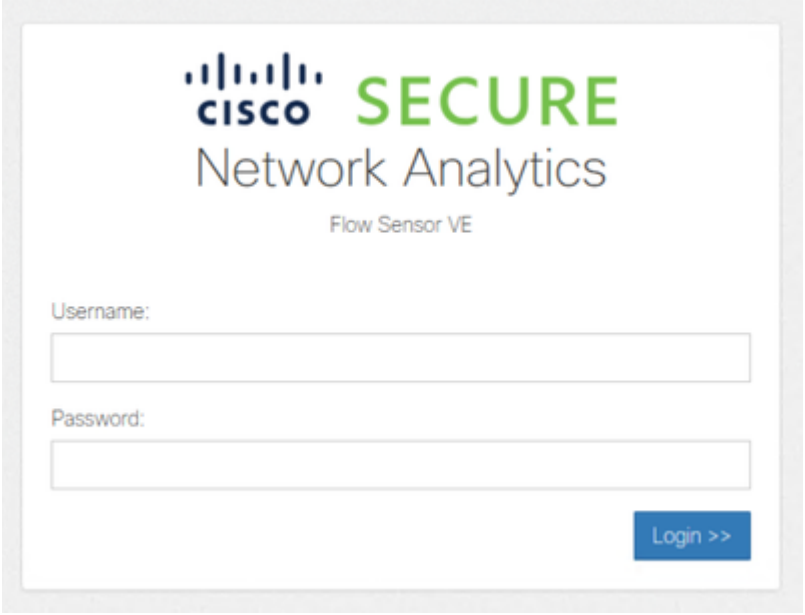
3. A browser tab opens for Central Management and shows the Inventory tab. From the Inventory tab, click the ellipsis icon for the appliance you wish to create a diagnostic pack for. Select View Appliance Statistics. Another new browser tab opens for that appliances Admin UI.



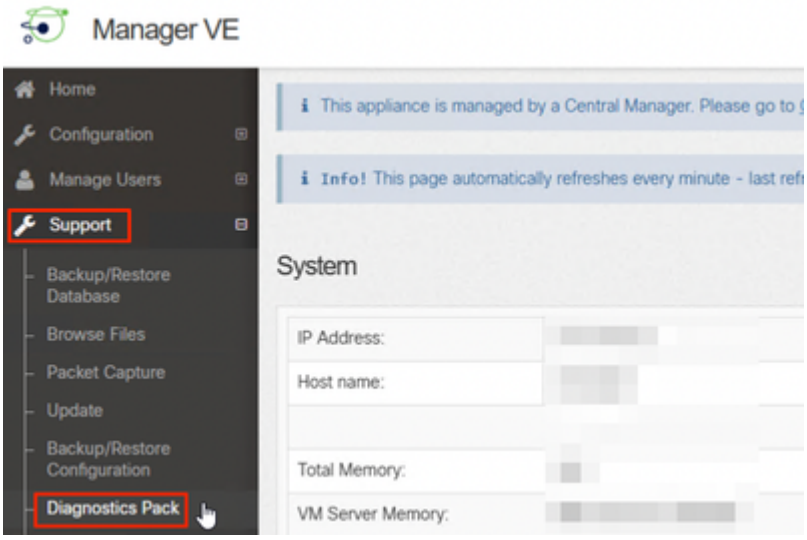
4. Log in to the appliance Admin UI with **admin** credentials. If you are not using the SNA Managers Central Management function, navigate to the log in page of the desired device via either its DNS resolvable FQDN or by its IP Address **https://{IP_or_FQDN_here}** and log in using the built in Admin user.

Note: To access the Managers Admin UI after logging in, change the URL: https://{Manager_IP_or_FQDN}/smc/index.html

---

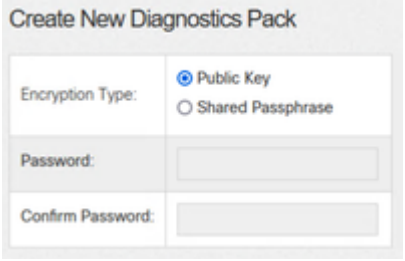


5. Click **Support** > **Diagnostics Pack** from the left menu.



6. Once in the Diagnostics Pack page, For Encryption Type either leave the default **Public Key** selected, or select **Shared Passphrase** and enter it in the **Password** and **Confirm Password** fields.

Note: Please provide shared passphrases to TAC in the file description field when you upload the Diagnostics pack to the Support Case Manager. Enter the description as a key:value pair with 'passphrase' being the key, and the value being set to the shared passphrase used to encrypt the file. Example: passphrase:<your_shared_passphrase>. This allows for the most effecient processing and analysis of the diagnostic bundle.



7. Select **Create Diagnostics Pack** to generate the diagnostics pack of the appliance. While it is being created, the focus is on a pop-up on the page.



8. Once finished, you are presented with a pop-up box which includes the **Download** button to download the Diagnostics Pack. Previously completed diagnostic packs can be downloaded from this page.



Note: If you do not have access to the Web UI, please use option **1. Via SystemConfig Menu**

Method 4. From Each Appliances Command Line Interface (CLI)

Note: This method is only available to users prior to software release 7.5.0.

There are times when it is not possible to generate the Diagnostics Pack of an appliance with the use of the previously described methods, however it can be generated directly from the Appliances CLI. The steps to complete this task are:

1. Connect to the desired SNA appliance via Secure Shell Protocol (SSH) or directly via console access.

Note: In case that you need to collect the diagnostics pack from a hardware appliance with no SSH access, the Kernel-based Virtual Machine (KVM) console from the Cisco Integrated Management Controller (CIMC) interface can be used as well.

2. Log in with **root** credentials.

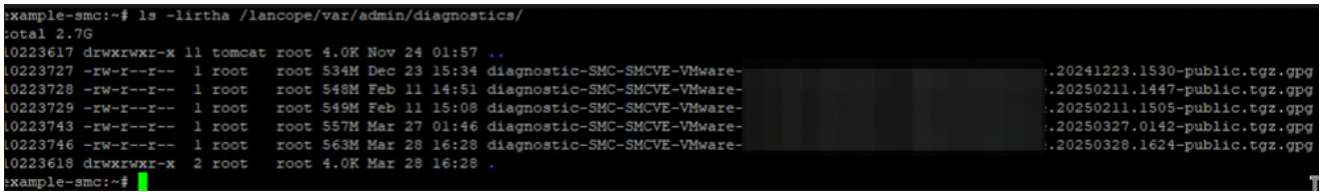
3. Run the commands for the SNA software release in use:

SNA software release 7.1.x to 7.3.x run the **doDiagPack** command.

SNA software release 7.4.x run the **diagnostics start** command.

4. Wait for the task to complete. On

5. The Diagnostics pack file is saved in the **/lancope/var/admin/diagnostics/** directory with a name scheme of "**diagnostic-<Device_type>-<Device_ID>.<YYYMMDD>.<HHMM>-*.tgz.gpg**"

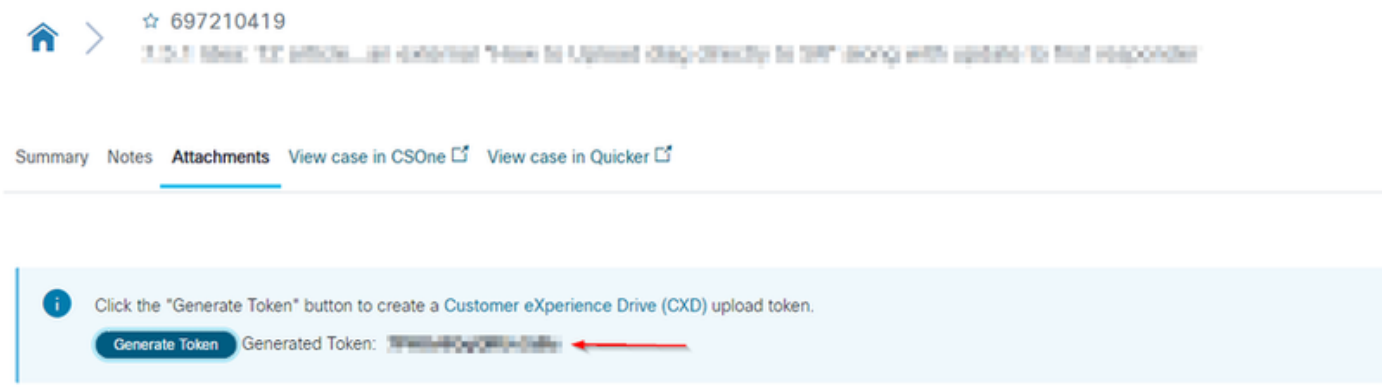


6. Transfer the generated file from the appliance to your local computer or to a file server with Secure Copy Protocol (SCP) or with a SSH File Transfer Protocol (SFTP) client like WinSCP.

Note: It is worth to mention that SNA software release 7.4.0 introduced a new feature that allows the Diagnostics Pack to be generated from the SystemConfig menu (CLI log in with **root** credentials > Enter **SystemConfig** > Navigate to **Recovery** > **Diagnostics Pack**).
For more information about this method, review the Secure Network Analytics System Configuration Guide 7.4.x.

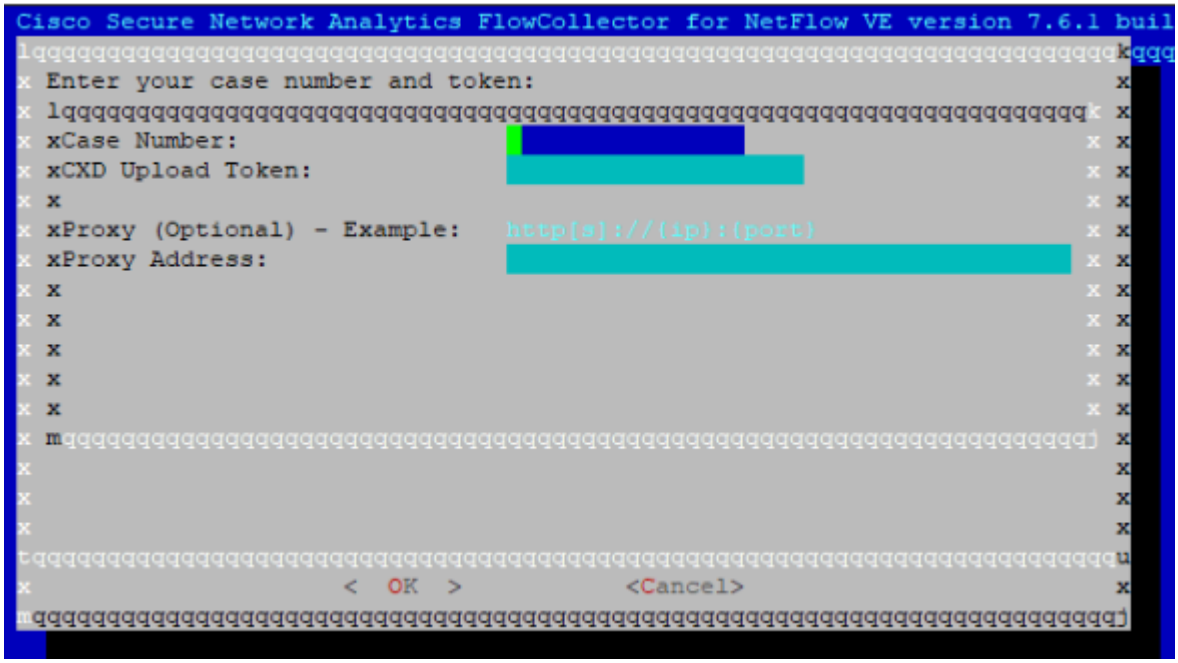
Generating a CXD Upload Token

- Access the Support Case Manager
- Access the support case in question and click on attachments
- Click the Generate Token button



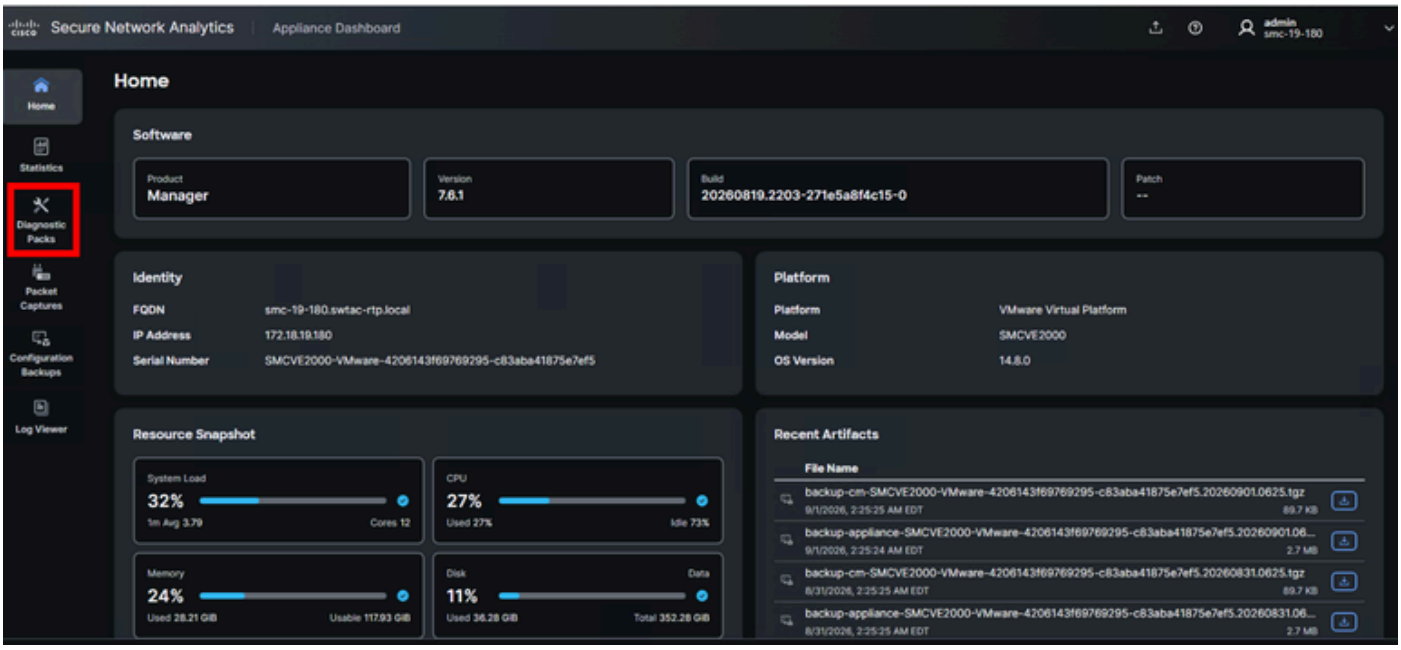
Using the upload token from within SystemConfig

- The generated token screen appears, this upload token can then be used from the SystemConfig -> Recovery -> Diagnostics -> Upload menu, in order to upload the diagnostic pack directory to the SR

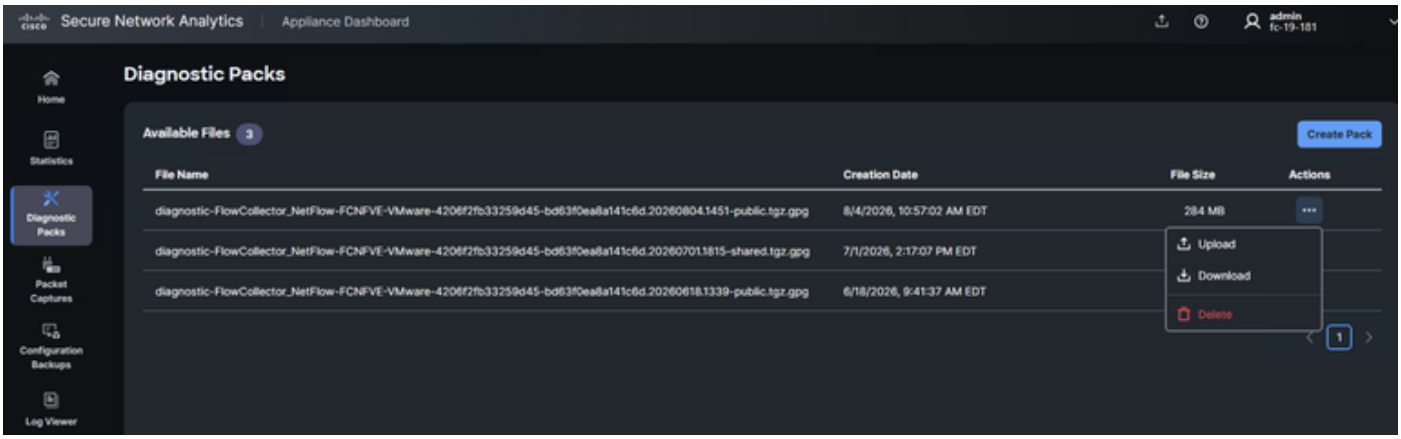


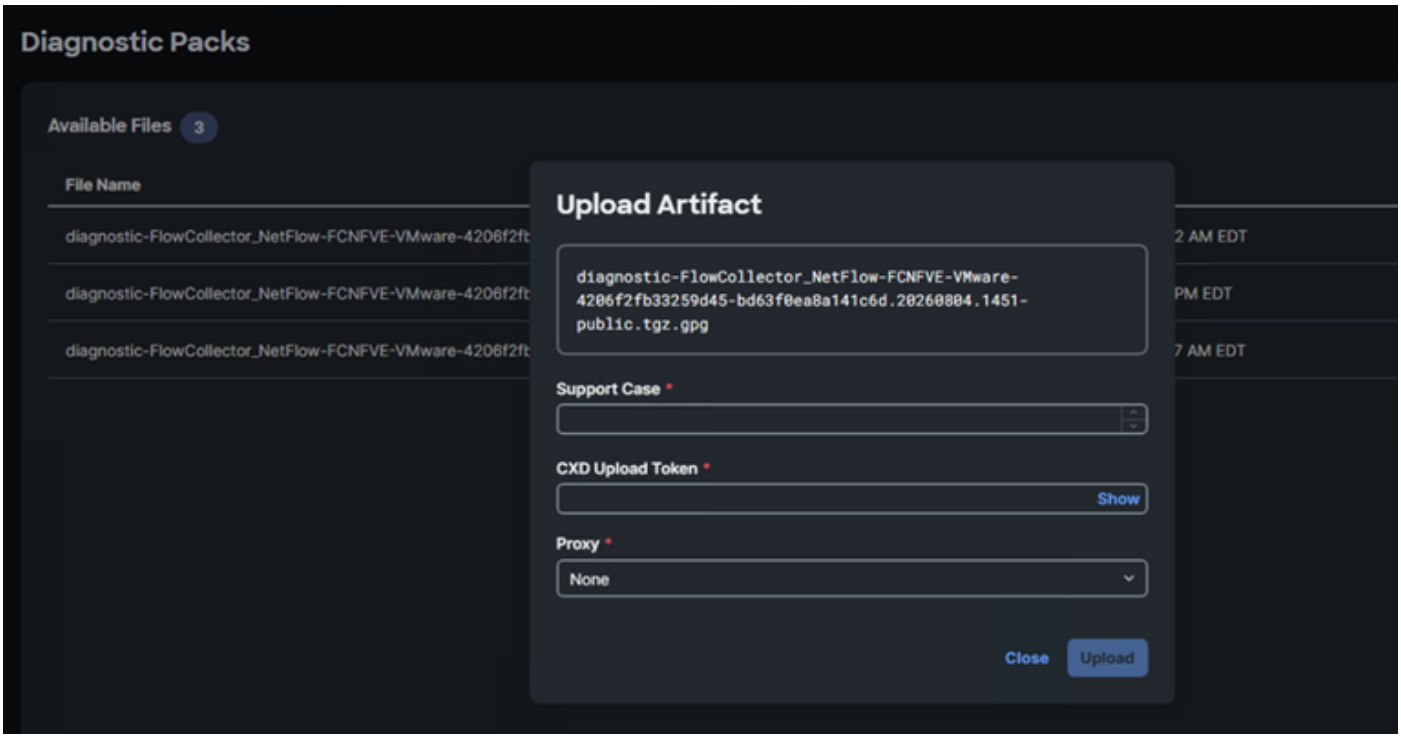
Use the upload token from within the SNA Web UI (new to 7.6.1)

- New to verison 7.6.1, you can not also upload the appliance diagnostic packs from the WebUI as well.
- Access the Central Manager Inventory page. (Configure -> Central Management -> Inventory)
- Under the Actions menu for the appliance that you wish to upload the diagnostic pack for, select "View Appliance Dashboard", and then select the interface (IPV4, IPV6, or Hostname) which you wish to access the device by. You are automatically passed through the one time password login and end up on the new Appliance Dashboard page.



From here, you can access the same "Upload" dialog





Troubleshoot

This section provides information you can use in order to troubleshoot failures generating diagnostic packs.

For Method 3, the error "There was an error creating the diagnostics pack. No files are available" appears after the **Create Diagnostics Pack** button is clicked in the Admin UI of an appliance if there is a permissions error or a specific directory is missing.



Steps to correct this error:

1. Log in to the appliance that has this behavior with **root** credentials via SSH.
2. Run the `ls -l /lancope/var/database/dbs/hsqldb/admin/` command to verify the content of the directory.

```
fcnf-cds:~# ls -l  /lancope/var/database/dbs/hsqldb/admin/
total 20
-rw-r--r-- 1 tomcat tomcat   16 Apr 28 00:38 admin.lck
-rw-r--r-- 1 tomcat tomcat    0 Apr 27 17:20 admin.log
-rw-r--r-- 1 tomcat tomcat   84 Apr 27 17:17 admin.properties
-rw-r--r-- 1 tomcat tomcat 2995 Apr 27 17:17 admin.script
drwxr-xr-x 2 tomcat tomcat 4096 Apr 27 17:20 admin.tmp
drwxr-xr-x 2 tomcat tomcat 4096 Jun  7  2021 backup
```

3. Ensure that the **backup** child directly exists and that its user/group owner is **tomcat**. If the **backup** child directory does not exist in the **/lancope/var/database/dbs/hsqldb/admin/** directory, it must be created and the correct ownership must be assigned. To create this directory, run the **install -d -m 0755 -o tomcat -g tomcat /lancope/var/database/dbs/hsqldb/admin** command.

4. Run the **ll /lancope/var/admin/** command to verify that the **backups** and **diagnostics** subdirectories exist and that their user/group owner is **root**.

```
fcnf-cds:~# ll /lancope/var/admin/
total 80
drwxrwxr-x 2 root root     4096 Apr 27 06:25 backups
drwxr-xr-x 2 root root     4096 Apr  7 21:39 cds
-rw-r--r-- 1 root root        0 Apr  6 22:10 clustered_database
drwxrwxr-x 2 root root     4096 Sep  7  2021 diagnostics
-rw-r--r-- 1 root root       40 Apr 27 17:18 hwserial
-rw-r--r-- 1 root root        8 Apr 27 17:18 meminfo
-rw-r--r-- 1 root root       69 Apr 27 17:18 model
-rw-r--r-- 1 root root       23 Apr 27 17:18 platform
drwxr-xr-x 3 root root     4096 Sep 15  2021 plugins
-rw-rw-rw- 1 root root        2 Apr 27 18:13 previous_engine_startup_mode
-rw-r--r-- 1 root root       47 Apr 27 17:18 serial
drwxr-xr-x 2 root root     4096 Apr  7 21:22 ssh
drwxr-xr-x 2 root root     4096 Apr  8 02:51 system.d
-rw-rw---- 1 root swadmin 12756 Apr  8 02:56 system.xml
drwxrwxrwx 2 root root     4096 Apr 28 00:25 tmp
drwxr-xr-x 2 root root     4096 Sep  7  2021 update
drwxrwxr-x 4 root tomcat   4096 Apr  8 02:49 upgrade
-rw-r--r-- 1 root root       36 Apr 27 17:18 uuid
```

5. If either of the **backups** and **diagnostics** subdirectories do not exist in the **/lancope/var/admin/** directory, they must be created with the relevant command:

    mkdir /lancope/var/admin/backups

    mkdir /lancope/var/admin/diagnostics

6. Once they have been created or verified to exist, try to generate the Diagnostics Pack of the SNA appliance again.

Related Information

For additional assistance, please contact Cisco Technical Assistance Center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts.

Technical Support & Documentation - Cisco Systems