

Generate Diagnostics Pack for Secure Network Analytics Appliances

Contents

[Introduction](#)

[Procedure](#)

[Method 1. From the Manager's Web User Interface \(UI\)](#)

[Method 2. From Each Appliance's Admin UI](#)

[Method 3. From Each Appliance's Command Line Interface \(CLI\)](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

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

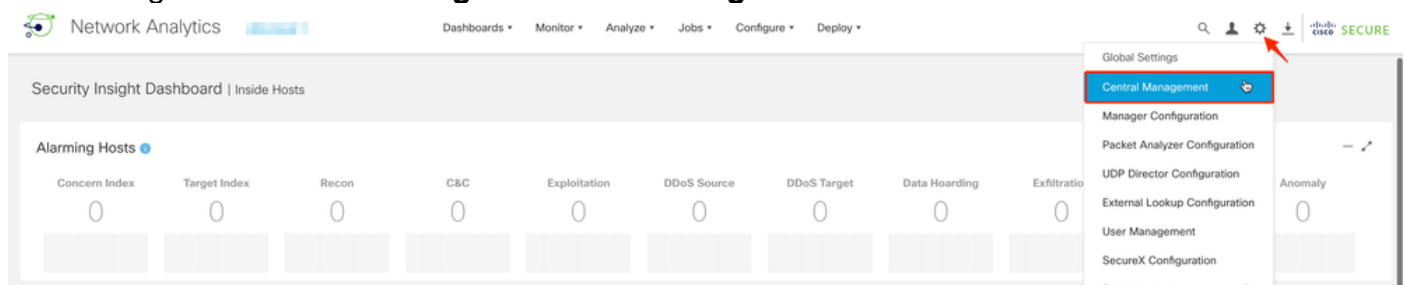
Procedure

There are three main methods to generate the Diagnostics Pack for the SNA appliances. The suggested method is **Method 1. From the Manager Web User Interface (UI)**, however the other two methods are an option in case that the Manager's Web UI is not available.

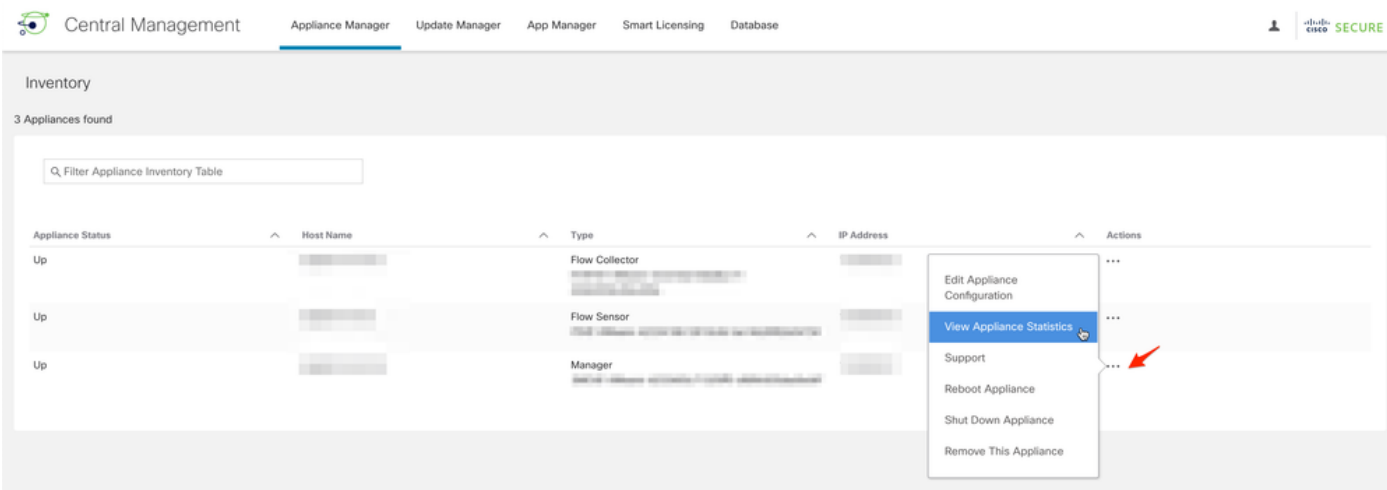
Note: If the Manager's Web UI is unavailable and you need to generate a Diagnostics Pack from the Manager, please refer to **Method 3. From Each Appliance's Command Line Interface (CLI)**.

Method 1. From the Manager's Web User Interface (UI)

1. Log in to the Manager's web UI.
2. Navigate to **Global Settings > Central Management**.



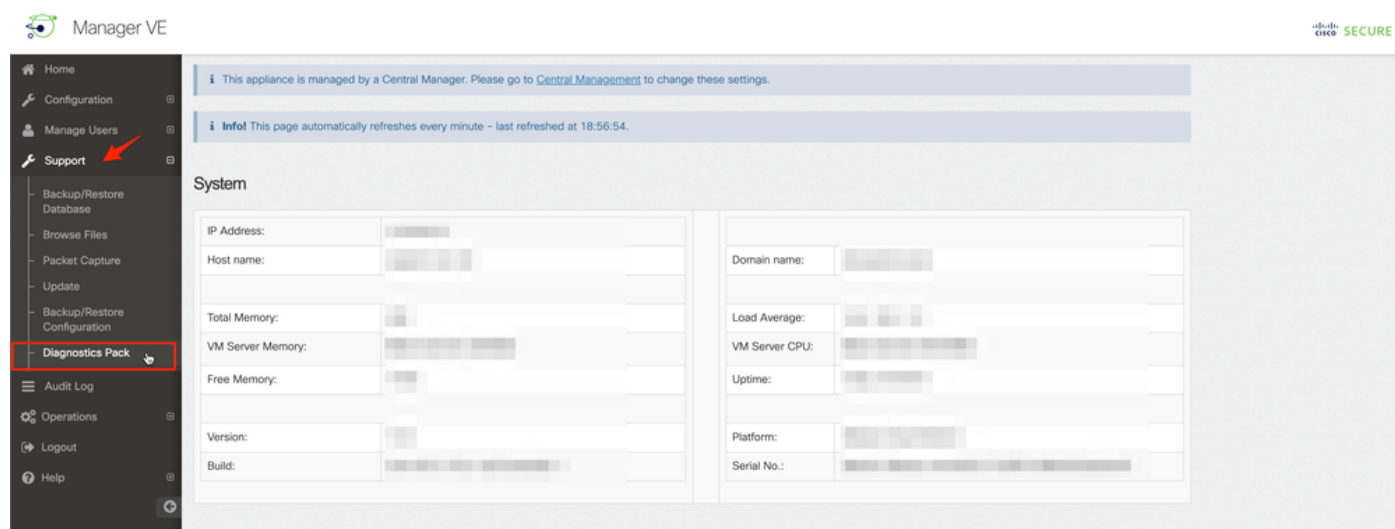
3. From the listed appliances locate the appliance from which you need to create the Diagnostics Pack and select **Actions (Ellipsis icon) > View Appliance Statistics**.



4. You must be redirected to the Admin UI of the selected appliance.

5. Log in to the appliance Admin UI with **admin** credentials.

6. From the menu on the left, navigate to **Support > Diagnostics Pack**.



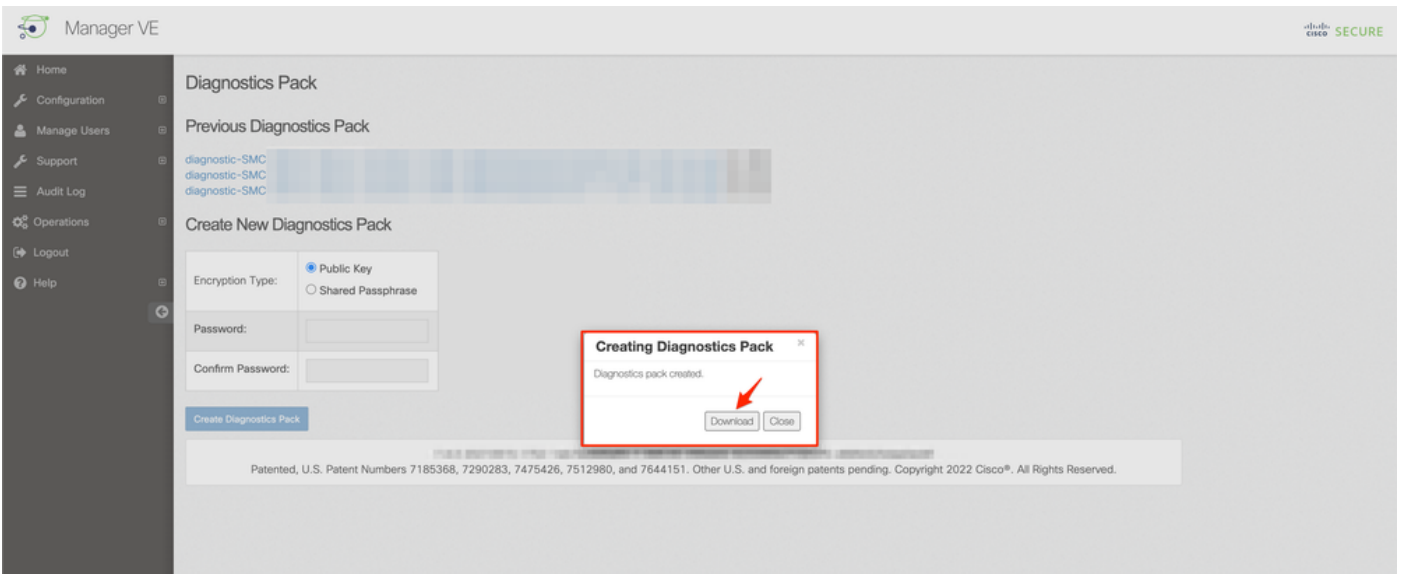
7. Once in the Diagnostics Pack page, you need to either select the default **Public Key** encryption or provide a shared key/passphrase to use for encryption.

Note: If you choose to use a custom key/password, then you must provide that passphrase in the file description when you upload the Diagnostics pack to the Support Case Manager.

8. Select **Create Diagnostics Pack** to generate the diagnostics pack of the appliance.



9. Once finished, you must be presented with a pop-up box which includes the **Download** button to download the Diagnostics Pack.



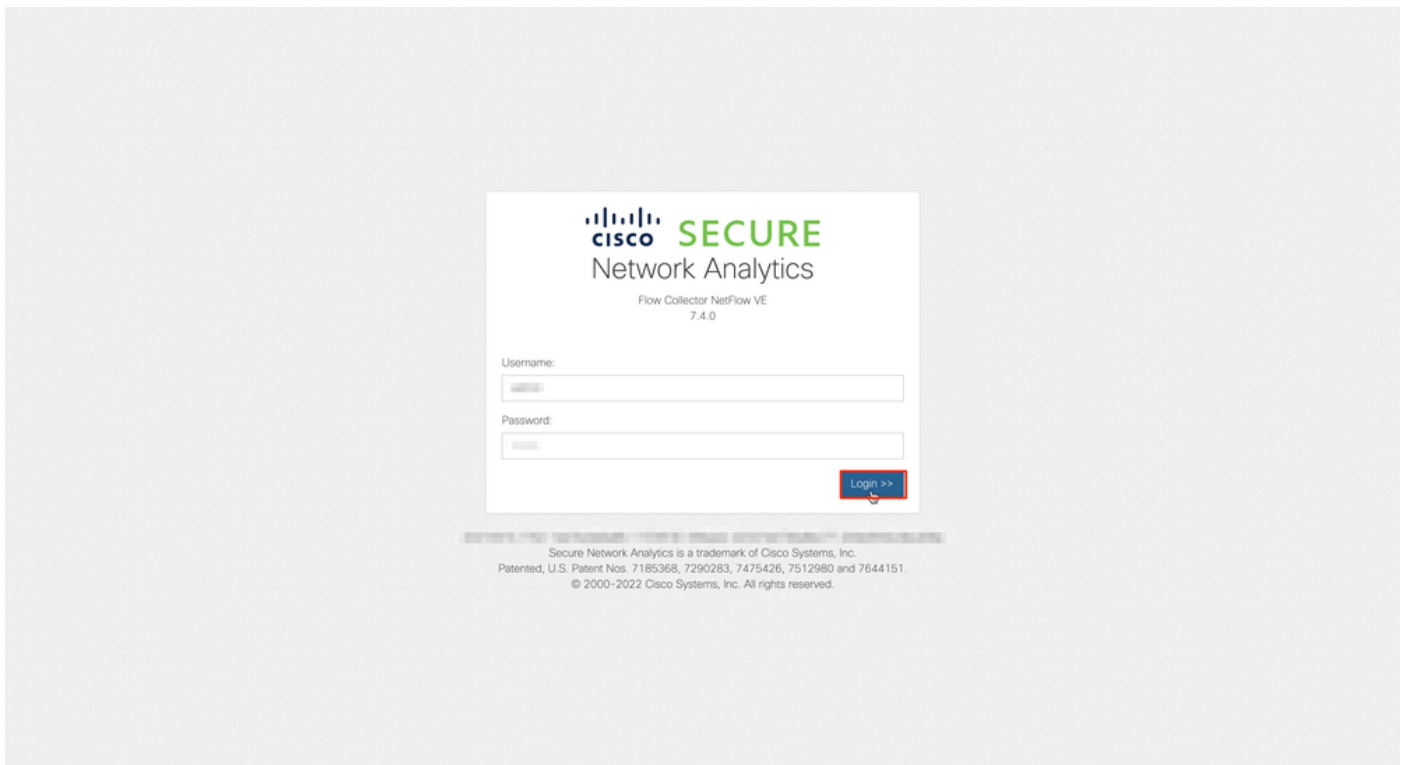
Method 2. From Each Appliance's Admin UI

For this method you must access to the appliance from which you want to generate the Diagnostics Pack, via Hypertext Transfer Protocol Secure (HTTPS).

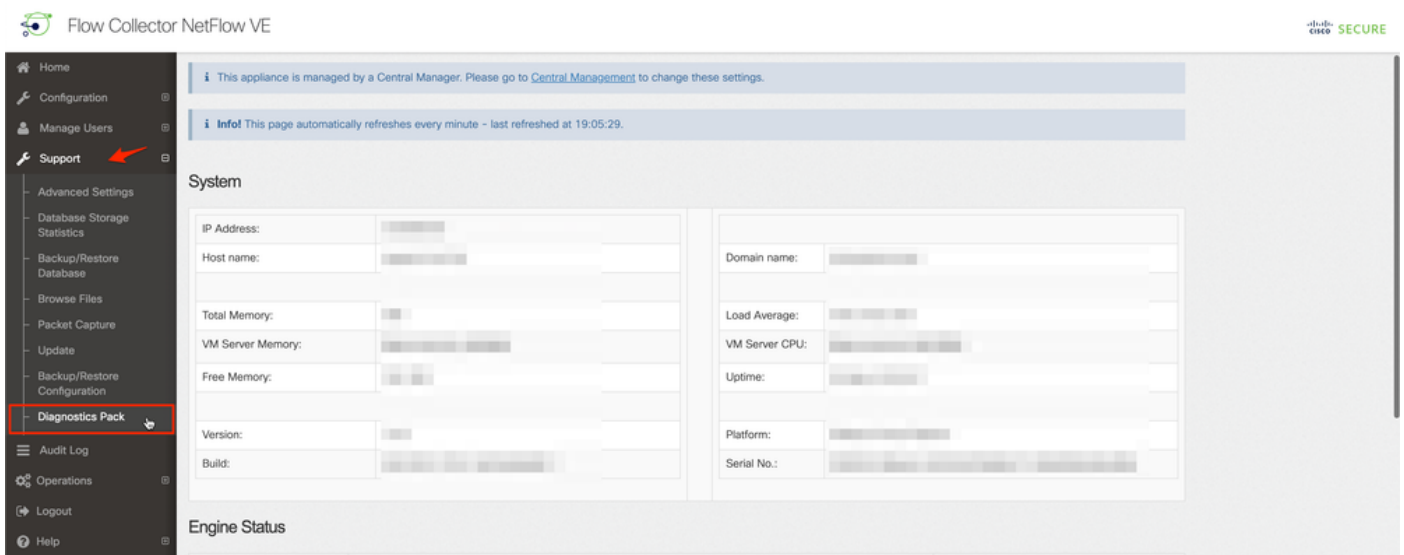
Note: To access directly to the Manager's **Admin UI** you must use the URL: https://<Manager_IP_address>/smc/index.html, otherwise you are redirected to the Manager's Web UI.

For example, in order to generate the Diagnostics Pack of a Flow Collector with this method you must follow the next steps:

1. From a web browser, navigate to **https://<FC_IP_address>**
2. Log in to the appliance Admin UI with admin credentials.



3. From the menu on the left, navigate to **Support > Diagnostics Pack**.



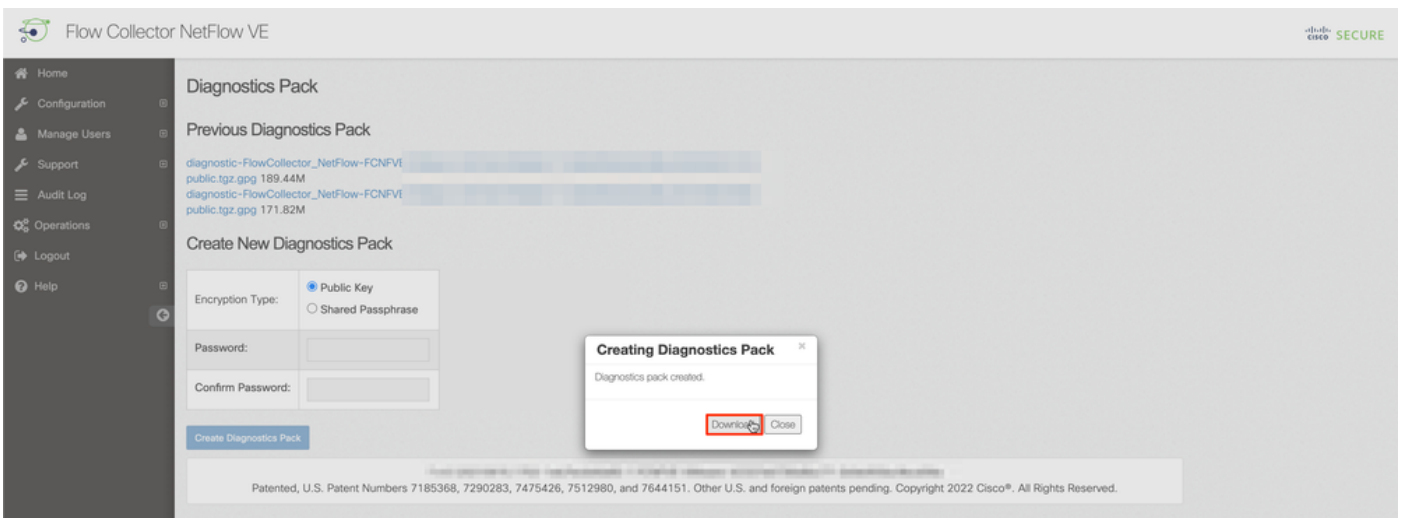
4. Once in the Diagnostics Pack page, you need to either select the default **Public Key** encryption or provide a shared key/passphrase to use for encryption.

Note: If you choose to use a custom key/passphrase, then you must provide that passphrase in the file description when you upload the Diagnostics pack to the Support Case Manager.

5. Select **Create Diagnostics Pack** to generate the diagnostics pack of the appliance.



6. Once finished, you must be presented with a pop-up box which includes the **Download** button to download the Diagnostics Pack.



Method 3. From Each Appliance's Command Line Interface (CLI)

There are some 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 appliance's 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. Enter one of the next commands (this depends on the version of SNA which is in use):

SNA version 7.1.x to 7.3.x

Enter the command **doDiagPack**

SNA version 7.4.x

Enter the command **diagnostics start**

4. Wait for the task to be completed.
5. Once the task has been completed, the Diagnostics pack file gets stored in the **/lancope/var/admin/diagnostics/** directory with a name scheme of "**diagnostic-
<Device_type>-<Device_ID>.<YYYYMMDD>.<HHMM>-* .tgz.gpg**"

```
smc:/# doDiagPack
smc:/# ls -l /lancope/var/admin/diagnostics/
total 32740
-rw-r--r-- 1 root root 33522766 Feb 24 02:29 diagnostic-SMC-SMCVE-VMware-4
        -6 .20220224.0227-public.tgz.gpg
smc:/# █
```

6. Copy 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. The diagnostics pack is located in the **/lancope/var/admin/diagnostics/** directory.

Note: It is worth to mention that SNA version 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](#).

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

There are some times when the creation of the Diagnostics Pack fails. The most common symptom is when you receive an error that reads "There was an error creating the diagnostics pack. No files are available" after the **Create Diagnostics Pack** button is clicked.



To correct this behavior, proceed as follows:

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.
3. Ensure that the **backup** subdirectory exists and that its user/group owner is **tomcat**.

```
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
```

If the **backup** subdirectory does not exist in the **/lancope/var/database/dbs/hsqldb/admin/** path, it must be created and the correct ownership must be assigned. For this, run these commands:

1. `mkdir /lancope/var/database/dbs/hsqldb/admin/backup`
2. `chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup`
4. Run the **ls -l /lancope/var/admin/** command to verify the content of the directory.
5. Ensure 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
fcnf-cds:~#
```

If one or none of the mentioned subdirectories do not exist in the **/lancope/var/admin/** path, they must be created and the correct ownership must be assigned. For this, run these commands:

1. `mkdir /lancope/var/admin/backups`
2. `mkdir /lancope/var/admin/diagnostics`

Once this has been verified, 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](#)