NSO Subscriber Microservices Infrastructure - Automation Function Pack Installation Guide, Release 2026.02

Cisco Confidential

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Copyright

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

Contents

1 Preface 4
2 Bias-free Documentation Policy 5
3 Before you begin 6
3.1 System requirements 6
3.2 Prerequisites 6
4 Installing NSO SMI Automation Function Pack 9
4.1 Performing NSO SMI Automation Function Pack system installation 9
4.2 Verifying the NSO SMI Automation Function Pack installation 12
5 Upgrade 14
5.1 Upgrading from SMF AFP 2026.01.0 to SMI AFP 2026.02.0 14
5.1.1 Preparing for Upgrade 14
5.1.2 Upgrading NSO from 6.4.8.1 to 6.4.8.2 16
5.1.3 Upgrading to SMI AFP v2026.02.0 on NSO v6.4.8.2 16
6 Uninstalling NSO SMI Automation Function Pack 21

1 Preface

Abstract

This ***Network Service Orchestrator Subscriber Microservices Infrastructure Automation Function Pack (NSO SMI AFP) Installation Guide*** includes information to help you install the NSO SMI AFP feature.

The NSO SMI AFP was previously known as NSO SMI CFP (Network Service Orchestrator Subscriber Microservices Infrastructure Core Function Pack).

Audience

This guide is intended for Cisco Advanced Services developers, network engineers, and system engineers who deliver the NSO SMI AFP functionalities to Cisco customers.

Additional Documentation

SL.No.	Documentation
1.	NSO Documentation
2.	NSO SMI AFP User Guide
3.	SMI Documentation

This document requires the reader to have a good understanding of Network Service Orchestrator. See the ***NSO User Guide*** for more information.

2 Bias-free Documentation Policy

Cisco follows a bias-free documentation policy. According to this policy, Cisco treats all persons with respect—regardless of race, color, ancestry, national origin, age, sex, citizenship, veteran status, marital status, sexual orientation, physical or mental ability, religious creed, or medical condition. Language or graphic elements that offend others violate our business philosophy and our company policy.

3 Before you begin

This section outlines the hardware requirements, software requirements, and the prerequisites to install NSO SMI AFP.

3.1 System requirements

NSO SMI AFP v2026.02.0 installation is supported on NSO v6.4.8.2.

The following table lists the hardware and software requirements to successfully install NSO SMI AFP.

Item	Requirement
Operating Systems	NSO and NSO SMI AFP are available for all Linux distributions and are tested on the following operating systems: • RHEL • Ubuntu • CentOS This documentation considers NSO SMI AFP installed on a single host running the Ubuntu server.
Software	• Java version 17 or higher • Python v3.12 or higher • OpenSSL, SSH, and ssh-pass
User account	User account must have **sudo** privileges.

3.2 Prerequisites

1. Make sure to have **sudo** privileges to perform the NSO SMI AFP installation. This user must also be part of the **ncsadmin** group. A **sudo** user has administrator privileges.
2. Perform a system installation of NSO v6.4.8.2 as per your requirement. For more information on the installation procedure, see the ***NSO Installation Guide***.

   Note: This documentation uses NSO v6.4.8.2 to demonstrate the CFP installation.
3. Make sure JDK-17 or higher is installed.
4. Make sure Python v3.12 or higher is installed.
5. Add ulimit level value for NSO in **/etc/init.d/ncs** as follows:

```
...
...
ncsdir=/opt/ncs/current
confdir=/etc/ncs
```

```
rundir=/var/opt/ncs
logdir=/var/log/ncs

ncs=${ncsdir}/bin/ncs
ulimit -n 65536
prog=ncs
conf="-c ${confdir}/ncs.conf"
heart="--heart"
...
...
```

6. Add and verify the ulimit value for the operating system. The following is an example to add the ulimit for CentOS operating system.
   - Edit the **/etc/security/limits.conf** file and add the following lines:

     ```
     * soft nproc 65535
     * hard nproc 65535
     * soft nofile 65535
     * hard nofile 65535
     ```

   - Run the `sysctl -p` script to set the parameters.
   - Log out of the system and log in again to apply the new values.
   - Verify the ulimit values are applied.

     ```
     $ ulimit -a
     core file size          (blocks, -c) 0
     data seg size           (kbytes, -d) unlimited
     scheduling priority             (-e) 0
     file size               (blocks, -f) unlimited
     pending signals                 (-i) 63407
     max locked memory       (kbytes, -l) 65536
     max memory size         (kbytes, -m) unlimited
     open files                      (-n) 65535
     pipe size            (512 bytes, -p) 8
     POSIX message queues     (bytes, -q) 819200
     real-time priority              (-r) 0
     stack size              (kbytes, -s) 8192
     cpu time               (seconds, -t) unlimited
     max user processes              (-u) 4096
     virtual memory          (kbytes, -v) unlimited
     file locks                      (-x) unlimited
     ```

7. (*Optional*) Create plan-notifications for the services in NSO and edit the **ncs.conf** file to add the **stream service-state-changes**.

   ```
   cisco@ncs(config)# services plan-notifications subscription
   <SAMPLE_NAME1> service-type smi:smi/smif:functions/smif:function
   component-type self state ready

   cisco@ncs(config)# services plan-notifications subscription
   <SAMPLE_NAME2> service-type smi:smi/smid:deployment component-type
   self state ready
   ```

   Edit the **/etc/ncs/ncs.conf** file as follows:

```
<!-- This is the builtin stream used by NCS to generate northbound --
>
      <!-- notifications for plan state transitions. -->
      <!-- See tailf-ncs-plan.yang -->

   <notifications>
    <event-streams>
      <stream>
        <name>service-state-changes</name>
        <description>Plan state transitions according to
        tailf-ncs-plan.yang</description>
        <replay-support>false</replay-support>
        <builtin-replay-store>
          <enabled>false</enabled>
          <dir>./state</dir>
          <max-size>S10M</max-size>
          <max-files>50</max-files>
        </builtin-replay-store>
      </stream>
```

8. Make sure to have set up a Cluster Manager (CM) to install and use NSO SMI AFP. For more information on how to install and set up a CM, see SMI device documentation.

4 Installing NSO SMI Automation Function Pack

You can perform NSO SMI AFP installation on NSO in two ways:

- System Installation
- Local Installation

The system installation, which is for a real-time production environment, is the preferred method of installation. The local installation is the demo version of the installation.

You must have **sudo** user privileges to perform the installation and run the installation commands. You can perform NSO SMI AFP System Installation on a single machine or multiple machines at a given time. System Installation is used for installation of NSO on multiple hosts/VMs from a Single Controller host.

This documentation describes how to perform NSO SMI AFP system installation. For information on local installation, contact your Cisco representative.

NOTE: AFP releases will follow the SMI/NF release versioning convention:

<YYYY>.RN.MN

Where,

- **YYYY** is a 4-digit year
- **RN** denotes the major Release Number
    - Always precedes with 0
    - Starts with 1
    - Resets to 1 after the last planned release of a year (YYYY)
- **MN** denotes the Maintenance Number
    - Starts with 0
    - Increments for every maintenance release
    - Resets to 0 at the beginning of every major release for that release

4.1 Performing NSO SMI Automation Function Pack system installation

This procedure uses NSO v6.4.8.2 to demonstrate the SMI AFP installation.

Note 1: Legacy NF NEDs are removed with the release of NSO SMI AFP v2026.02.0. This change does not have impact on AFP functionality.

Note 2: Ensure that the SMI NED is loaded for AFP to function correctly.

1. Log on to the host machine as the **sudo** user.
2. Check the NSO installation.

```
$ cd ~
$ ncs --version
6.4.5.1
$ which ncs
/opt/ncs/current/bin/ncs
```

3. Obtain and download the **ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz.SSA.tgz** package from Cisco website and copy it to the host server.
4. Extract the file and verify the image.
   a. Extract the **ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz.SSA.tgz** file.

      The following is an example of commands in the Linux environment.

```
$ mkdir 6.1_2026.02.0_release_files
$ tar zxvf ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz.SSA.tgz --
directory 6.1_2026.02.0_release_files
$ cd 6.1_2026.02.0_release_files
```

   b. To verify the image, use the following command:

```
$ python cisco_x509_verify_dev.py -e SMI-NSO_DEV_KEY-CCO_DEV.cer -i
ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz -s ncs-6.4.8.2-nso-smi-
afp-2026.02.0.tar.gz.signature.SSA -v dgst -sha512 -k dev --CAfile
trca.cer --SubCAfile Innerspace_DEV.cer
```

      For more information, refer to the **ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz.SSA.README file** attached with **ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.SSA.tgz**.

   c. If you skip verification, ensure that the software is authentic before you skip verification.
5. Extract the TAR file to the current directory. If the folder already exists, be sure to create a backup of the existing folder.

```
$ tar -vxf ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz
$ cd ncs-6.4.8.2-nso-smi-afp-2026.02.0

The following packages are extracted:
ncs-6.4-etsi-sol003-1.13.19.tar.gz
ncs-6.4-openstack-cos-4.2.34.tar.gz
ncs-6.4.3-resource-manager-4.2.10.tar.gz
ncs-6.4.8-cisco-staros-5.57.5.tar.gz
ncs-6.4.8.2-cisco-etsi-nfvo-4.7.8-fcdb6b99-2026-01-06.tar.gz.tar.gz
ncs-6.4.8.2-cisco-smi-deployer-2026.02.0.tar.gz
```

```
ncs-6.4.8.2-dvpc.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-esc-5.3.0.94.tar.gz
ncs-6.4.8.2-mobility-common.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mobility-mop.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mobility-rcm-subscriber.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mop-common.tar.gz-2026.02.0.tar.gz
```

Stop NCS, copy the SMI packages to the NSO package directory, and restart NCS with the package-reload option.

Note 1: If you are not deploying DVPC or using AFP for configuration management, do not copy the packages associated with those components.

Note 2: DVPC functionality is currently unavailable in the 2026.02.0 release due to recent updates within the MSUP/EPCGW Ops Center. Please refer to the Release Notes for the latest status and any required configuration updates.

```
ncs-6.4.8.2-mobility-common.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mobility-mop.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mobility-rcm-subscriber.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mop-common.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-dvpc.tar.gz-2026.02.0.tar.gz
```

```
$ sudo /etc/init.d/ncs stop
$ cd ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz
$ sudo cp * /var/opt/ncs/packages
$ sudo /etc/init.d/ncs restart-with-package-reload
```

The NSO SMI AFP system installation is now complete.

6. Load merge kickers as follows:
   Prerequisite: You must load merge the following payload on installation of 2026.02.0. To load merge the package, you need to add hide-group “debug” to NSO.
   a. Stop NSO.
   b. Edit the ncs.conf file and append the following information.
      The user must add “debug” into <unhide-group> in the ncs.conf file.

      ```
      <unhide-group> <name>debug</name> </unhide-group>
      ```

   c. Restart NSO.
   d. From the CLI mode, run the following command:

      ```
      user@ncs# configure
      user@ncs(config)# unhide debug
      ```

e. Manually load merge the following payload for kickers. You must perform this task for Cisco-smi-deployer to deploy the services correctly.

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <kickers xmlns="http://tail-f.com/ns/kicker">
    <data-kicker>
      <id>cisco-smi-internal-sync-run</id>
      <monitor>/smi:smi/smii:internal/cluster-manager-
plan/result/clusters/internal/sync-triggers</monitor>
      <kick-node>/smi:smi/smii:internal/cluster-manager-
plan[name=current()/../../../../name]/result/clusters[name=current(
)/../../name]/internal</kick-node>
      <action-name>sync-run-kicker</action-name>
    </data-kicker>
    <data-kicker>
      <id>cisco-smi-internal-sync-status</id>
      <monitor>/smi:smi/smii:internal/cluster-manager-
plan/result/clusters/sync-status</monitor>
      <kick-node>/smi:smi/smii:internal/cluster-manager-
plan[name=current()/../../../../name]/result/clusters[name=current()/.
./name]/internal</kick-node>
      <action-name>update-sync</action-name>
    </data-kicker>
    <data-kicker>
      <id>cisco-smi-deployment-drain-status</id>
      <monitor>/smi:smi/smid:deployment-plan/result/cluster-
result/node-result/node-status</monitor>
      <kick-
node>/smi:smi/smid:deployment[name=current()/../../../../name]/clus
ters/cluster[name=current()/../../cluster]/node[name=current()/../n
ode]</kick-node>
      <action-name>update-drain</action-name>
    </data-kicker>
  </kickers>
</config>
```

4.2 Verifying the NSO SMI Automation Function Pack installation

Use the information in this section to view the build information, package version, and package status to verify the NSO SMI AFP system installation.

To verify the NSO SMI Automation Function Pack installation:

1. Verify the package version and status.

```
luser@ncs# show packages package package-version | tab
NAME                    PACKAGE VERSION
-------------------------------------------------------
cisco-chaos-nc-1.0      1.0
cisco-etsi-nfvo         4.7.8
cisco-smi-deployer      2026.02.0
cisco-smi-dvpc          2026.02.0
cisco-smi-nc-1.1        1.1.2026.02.1
cisco-staros-cli-5.57   5.57.5
esc                     5.3.0.94
```

```
etsi-sol003-gen-1.13      1.13.19
mobility-common           2026.02.0
mobility-rcm-subscriber   2026.02.0
mop-automation            2026.02.0
mop-common                2026.02.0
openstack-cos-gen-4.2     4.2.34
resource-manager          4.2.10
```

2. Verify the packages are loaded correctly.

   luser@ncs# show packages package oper-status | tab

```
NAME                 UP  PROGRAM  JAVA          PYTHON        BAD  PACKAGE PACKAGE CIRCULAR  PACKAGE   FILE  ERROR WARNINGS
                         CODE     UNINITIALIZED UNINITIALIZED NCS  NAME    VERSION DEPENDENCY META DATA LOAD  INFO
                         ERROR                                VERSION                      ERROR     ERROR
-------------------------------------------------------------------------------------------------------------------------
---
cisco-chaos-nc-1.0       X  -        -             -             -    -       -       -          -         -     -     -
cisco-etsi-nfvo          X  -        -             -             -    -       -       -          -         -     -     -
cisco-smi-deployer       X  -        -             -             -    -       -       -          -         -     -     -
cisco-smi-dvpc           X  -        -             -             -    -       -       -          -         -     -     -
cisco-smi-nc-1.1         X  -        -             -             -    -       -       -          -         -     -     -
cisco-staros-cli-5.57    X  -        -             -             -    -       -       -          -         -     -     -
esc                      X  -        -             -             -    -       -       -          -         -     -     -
etsi-sol003-gen-1.13     X  -        -             -             -    -       -       -          -         -     -     -
mobility-common          X  -        -             -             -    -       -       -          -         -     -     -
mobility-rcm-subscriber  X  -        -             -             -    -       -       -          -         -     -     -
mop-automation           X  -        -             -             -    -       -       -          -         -     -     -
mop-common               X  -        -             -             -    -       -       -          -         -     -     -
openstack-cos-gen-4.2    X  -        -             -             -    -       -       -          -         -     -     -
resource-manager         X  -        -             -             -    -       -       -          -         -     -     -
```

5 Upgrade

5.1 Upgrading from SMF AFP 2026.01.0 to SMI AFP 2026.02.0

Perform the following tasks in the order listed to upgrade SMI CFP to version 2026.02.0 on NSO v6.4.8.2:

1. Preparing for Upgrade
2. Upgrading NSO from 6.4.8 1 to 6.4.8.2
3. Upgrading to SMI AFP v2026.02.0 on NSO v6.4.8.2

5.1.1 Preparing for Upgrade

To prepare the system to upgrade to SMI v2026.02.0:

1. Verify the current service plan status of zombies, deployment plan, function plan, and application plan if applicable.

```
user@ncs> show zombies

user@ncs> show smi deployment-plan
user@ncs> show smi functions function-plan
user@ncs> show smi applications application-plan upf
```

2. Ensure that there are no active syncs running on any cluster manager.
3. Disable the NSO HA cluster, if applicable.

   If you have NSO HA packages or NSO HA cluster installed, disable HA in the NSO command line and in the NCS configuration file. For more information, see the NSO documentation to disable NSO HA cluster for all NSO HA cluster nodes, starting from active nodes followed by all standby nodes.

   NOTE: You must follow the same procedure to upgrade all NSO HA cluster nodes starting from active node.

```
### Make sure your /etc/ncs/ncs.conf has completely disabled ha
vi /etc/ncs/ncs.conf
=======================
   <ha>
     <enabled>false</enabled>
   </ha>
=======================
```

4. Back up the current NSO-SMI environment on the current version.

   If the upgrade is not completed, it is easy to recover later.

```
$ sudo -s
# source /etc/profile.d/ncs.sh
# /etc/init.d/ncs stop
# ncs-backup
```

```
# exit
$
```

5. Delete or disable the notifications subscription in one of the following ways:

   Start the NCS process using the following command:

   ```
   $ sudo /etc/init.d/ncs start
   ```

   a. Save the notifications subscription first and then delete it. This helps to recover the notifications subscription after the upgrade process.

      i. Save the notifications subscription.

      ```
      $ ncs_load -p "/devices/device/notifications/subscription" -F
      p > netconf_streams.xml
      ```

      ii. Delete the notifications subscription.

      ```
      user@ncs# configure
      user@ncs(config)# no devices device * notifications
      subscription
      user@ncs(config)# commit dry-run
      user@ncs(config)# commit
      ```

   b. Disable notifications subscriptions.

   ```
   user@ncs# devices device * notifications subscription download-
   status disconnect

   user@ncs# devices device * notifications subscription node-state
   disconnect

   user@ncs# devices device * notifications subscription node-status
   disconnect

   user@ncs# devices device * notifications subscription sync-state
   disconnect

   user@ncs# devices device * notifications subscription sync-status
   disconnect

   user@ncs# devices device * notifications subscription vm-state
   disconnect

   user@ncs# devices device * notifications subscription alert-
   notification disconnect

   admin@ncs# devices device * notifications subscription system-
   status disconnect

   admin@ncs# devices device * notifications subscription system-
   upgrade disconnect
   ```

6. Log on to the host machine as the **sudo** user.

Ensure to have the NSO SMI installation tar ball or bin file ready on your system.

7. Download the ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz.SSA.tgz file from the Cisco website and copy it to the host server.

5.1.2 Upgrading NSO from 6.4.8.1 to 6.4.8.2

1. Install the new NSO version.

   ```
   $ sudo sh nso-NEWVERSION.OS.ARCH.installer.bin --system-install
   ```

2. Change to Super User privileges.

   ```
   $ sudo -s
   ```

3. Stop the previously installed NSO version.

   ```
   # /etc/init.d/ncs stop
   ```

4. Backup the data completely for disaster recovery. Ensure that you have stopped NSO.

   The output of the file name must be noted for later use during recovery.

   ```
   # ncs-backup
   ```

5. Switch to the new version by updating the symbolic link.

   ```
   # cd /opt/ncs
   # rm -f current
   # ln -s ncs-NEWVERSION current
   ```

   NOTE: After the CFP package is upgraded, you can start NCS as per Step 4 of Section 5.1.3.

   Refer to the **NSO Installation Guide** for details on the upgrade procedure from 6.4.8.1 to 6.4.8.2

5.1.3 Upgrading to SMI AFP v2026.02.0 on NSO v6.4.8.2

1. From **/var/opt/ncs/packages**, remove cisco-smi-deployer and other dependent packages that are upgraded in 2026.01.0. See Step 3 in this procedure for the list of packages.

   ```
   $ sudo -s
   # cd /var/opt/ncs/packages/
   # rm ncs-6.4.8.2-cisco-smi-deployer-2026.01.0.tar.gz
   ```

   Extract the content of the **ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz.SSA.tgz** file to the current directory. For more information, refer to step 4 in Section 4.1.

2. Extract the TAR file to the current directory. If the folder already exists, be sure to create a backup of the existing folder.

```
$ tar -vxf ncs-6.4.8.2-cisco-smi-deployer-2026.02.0.tar.gz
$ cd ncs-6.4.8.2-nso-smi-afp-2026.02.0
$ pwd
Copy ncs-6.4.8.2-nso-smi-afp-2026.02.0/* to /var/opt/ncs/packages and
other required packages
```

Note: If you are not deploying the Mobility Services User Plane or the Mobility Service Control Plane you do not need to copy over the dvpc package.

The following packages are extracted:

```
ncs-6.4-etsi-sol003-1.13.19.tar.gz
ncs-6.4-openstack-cos-4.2.34.tar.gz
ncs-6.4.3-resource-manager-4.2.10.tar.gz
ncs-6.4.8-cisco-staros-5.57.5.tar.gz
ncs-6.4.8.2-cisco-etsi-nfvo-4.7.8-fcdb6b99-2026-01-06.tar.gz.tar.gz
ncs-6.4.8.2-cisco-smi-deployer-2026.02.0.tar.gz
ncs-6.4.8.2-dvpc.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-esc-5.3.0.94.tar.gz
ncs-6.4.8.2-mobility-common.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mobility-mop.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mobility-rcm-subscriber.tar.gz-2026.02.0.tar.gz
ncs-6.4.8.2-mop-common.tar.gz-2026.02.0.tar.gz
```

Edit the **ncs.conf** file to remove the following information. If you must retain the <large-scale> information, see the NSO documentation to understand its location in the **ncs.conf** file.

```
<show-log-directory> ${NCS_LOG_DIR}</show-log-directory>

<large-scale>
    <lsa>
      <!-- Enable Layered Service Architecture, LSA. This requires
           a separate Cisco Smart License.
      -->
      <enabled>false</enabled>
    </lsa>
  </large-scale>
```

3. Stop NSO, copy the packages from the packages directory, and restart NSO with the **package-reload** option.

```
$ sudo /etc/init.d/ncs stop
$ cd /home/$USER/ncs-6.4.8.2-cisco-smi-deployer-2026.02.0
#Copy the cisco-smi-deployer package or other dependent packages which
needs to be loaded
$ sudo cp ncs-6.4.8.2-nso-smi-afp-2026.02.0.tar.gz
/var/opt/ncs/packages
```

```
$ sudo /etc/init.d/ncs restart-with-package-reload
```

4. Verify the packages are up and running.

```
user@ncs# show packages package package-version
user@ncs# show packages package oper-status
```

6. Update the following device configurations.

   Set ssh-algorithms to ssh-rsa for all the deployed services and global settings.

```
user@ncs# set devices global-settings ssh-algorithms public-key ssh-
rsa
user@ncs# commit
### For each deployed devices
user@ncs# set devices device <Device_Name> ssh-algorithms public-key
ssh-rsa
user@ncs# commit
```

7. Depending on how you have deleted or disabled the notification streams, perform one of the following tasks:

   a. If you deleted Netconf notification subscriptions as mentioned in **Step 7a** in section **Preparing for Upgrade**, create the Netconf notification subscriptions as follows:

```
user@ncs(config)# load merge netconf_streams.xml
user@ncs# commit
```

   b. Add xpath filtering to devices subscriptions to ignore the notifications that are not required:

```
nsoadmin@ncs(config)# devices device * notifications
subscription system-status xpath not(//system-helm-update-
notification)
Value for 'stream' (<string>): system-status
Value for 'local-user' (<string>): <your-nso-local-user-name>

nsoadmin@ncs(config-subscription-system-status)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.

nsoadmin@ncs(config)# devices device * notifications
subscription alert-notification xpath "not(//alert-
label[name='alertname' and value='watchdog'])"
Value for 'stream' (<string>): alert-notification
Value for 'local-user' (<string>): <your-nso-local-user-name>

nsoadmin@ncs(config-subscription-alert-notification)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

   c. If you deleted or disabled notifications as mentioned in **Step 7b** in section **Preparing for Upgrade**, enable the Netconf notification subscriptions as follows:

```
user@ncs# devices device * notifications subscription download-
status reconnect

user@ncs# devices device * notifications subscription node-state
reconnect

user@ncs# devices device * notifications subscription node-status
reconnect

user@ncs# devices device * notifications subscription sync-state
reconnect

user@ncs# devices device * notifications subscription sync-status
reconnect

user@ncs# devices device * notifications subscription
vm-state reconnect

user@ncs# devices device * notifications subscription alert-
notification reconnect

user@ncs# devices device * notifications subscription system-status
reconnect

user@ncs# devices device * notifications subscription system-
upgrade reconnect
```

8. If you require to upgrade the image and NED versions, see section ***Upgrading CNFs*** in the **NSO SMI AFP User Guide**. To upgrade only the NED versions, see section ***Migrating NED Versions*** in the **NSO SMI AFP User Guide**.
9. After the upgrade is complete, every service is in the same state as it was prior to upgrading. Be sure to fix any **not-ready** or **failed** services.

   If any errors or failures occur, restore the NSO backup environment. For more information about how to restore the NSO backup, see the ***NSO Administration Guide***.

   Note: Before attempting to upgrade again, analyze the logs to understand the cause of the failures.
10. If NSO HA package was installed, recover the NSO HA cluster. For more information, see the NSO documentation.
11. Load merge kickers as follows:
    a. Modify the ncs.conf file to append the following information. The user must add “debug” into <unhide-group> in the ncs.conf file.

       ```
       <unhide-group> <name>debug</name> </unhide-group>
       ```

    b. Restart NCS.

       ```
       sudo /etc/init.d/ncs restart
       ```

    c. From the CLI mode, run the following command:

```
user@ncs# configure
user@ncs(config)# unhide debug
```

d. In the same NCS session, load merge the kickers manually.

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <kickers xmlns="http://tail-f.com/ns/kicker">
    <data-kicker>
      <id>cisco-smi-internal-sync-run</id>
      <monitor>/smi:smi/smii:internal/cluster-manager-
plan/result/clusters/internal/sync-triggers</monitor>
      <kick-node>/smi:smi/smii:internal/cluster-manager-
plan[name=current()/../../../../name]/result/clusters[name=current(
)/../../name]/internal</kick-node>
      <action-name>sync-run-kicker</action-name>
    </data-kicker>
    <data-kicker>
      <id>cisco-smi-internal-sync-status</id>
      <monitor>/smi:smi/smii:internal/cluster-manager-
plan/result/clusters/sync-status</monitor>
      <kick-node>/smi:smi/smii:internal/cluster-manager-
plan[name=current()/../../../name]/result/clusters[name=current()/.
./name]/internal</kick-node>
      <action-name>update-sync</action-name>
    </data-kicker>
    <data-kicker>
      <id>cisco-smi-deployment-drain-status</id>
      <monitor>/smi:smi/smid:deployment-plan/result/cluster-
result/node-result/node-status</monitor>
      <kick-
node>/smi:smi/smid:deployment[name=current()/../../../../name]/clus
ters/cluster[name=current()/../../cluster]/node[name=current()/../n
ode]</kick-node>
      <action-name>update-drain</action-name>
    </data-kicker>
  </kickers>
</config>
```

Load merge the kickers using the following command:

```
user@ncs(config)# load merge kicker.xml
user@ncs(config)# commit
```

The SMI AFP upgrade process is now complete.

6 Uninstalling NSO SMI Automation Function Pack

Before you uninstall NSO SMI AFP, delete all the services, remove the devices from the NSO device tree, and remove any dependent packages.

For more information on how to delete the services, see the **NSO SMI AFP User Guide**.

Note: If you are using Config management (mop-common, mobility-common, mobility-mop) packages, you need to remove configuration and operational data related to these packages. For more information contact Cisco representative.

To uninstall NSO SMI Automation Function Pack:

1. Remove the SMI AFP packages from the **/var/opt/ncs/packages** directory.
2. Reload the packages in NSO.

```
$ ncs_cli -Cu $USER
cisco@ncs# packages reload force
```

This page is intentionally left blank.