Integrate Cisco NSO

This chapter contains the following topics:

- NSO integration workflow, on page 1
- Configure standalone NSO, on page 2
- Configure Cisco NSO for Layered Service Architecture, on page 7
- Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 12
- Install NSO function packs manually, on page 20
- Configure JSON Web Token authentication for NSO, on page 20

NSO integration workflow

Cisco Crosswork Network Controller supports Cisco Network Services Orchestrator (Cisco NSO) as a standalone deployment or as a Layered Service Architecture (LSA) deployment.

You select the deployment type when you install NSO. Use the standalone NSO workflow for a standalone NSO deployment. Use the LSA NSO workflow for an NSO deployment that uses customer-facing service (CFS) and resource-facing service (RFS) nodes.

These stages describe the NSO integration workflow:

1. Install a compatible Cisco NSO version. For compatibility details, see the *Release Notes for Crosswork Network Controller, Release 7.2.1 SP* for your Crosswork Network Controller release. For installation instructions, see Cisco NSO documentation.
2. Configure the NSO access-control settings that Crosswork uses for role-based access control and Device Access Groups.
3. Add the NSO provider in Crosswork. Use the standalone provider properties for standalone NSO, and use the LSA provider properties for LSA NSO.
   - For standalone NSO, see Configure standalone NSO.
   - For LSA NSO, see Configure Cisco NSO for Layered Service Architecture.
4. Edit the provider policy details if the default device-addition policy does not match your environment.
5. Install the required Cisco NSO function packs. For more information, see Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 12 (recommended) or Install NSO function packs manually, on page 20.

Note

- The NSO core function packs are bundled in the *cnc-function-packs-7.2.1.signed.bin* file.
- The Cisco Crosswork Network Controller Function Pack SDK Application (*cnc-function-pack-sdk-7.2.1-bin.zip.tar.gz*) is also available for download on cisco.com. The SDK provides tools and source-code examples you can use to develop, build, package and deploy the TSDN function pack on Crosswork Network Controller.

6. Configure JSON Web Token (JWT) authentication between Crosswork and NSO.

Configure standalone NSO

Use this workflow when your Crosswork deployment uses standalone Cisco NSO.

Before you begin

- Install a compatible Cisco NSO version.
- Create the Crosswork credential profile that you will use for the NSO provider.
- Know the NSO server IP address or fully qualified domain name (FQDN) and the Network Element Driver (NED) device models and driver versions used in your topology.

Procedure

Step 1 Enable service-level NETCONF Access Control Model (NACM) on the standalone NSO server.

Example:

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

Step 2 Create the NACM group before you create the rule list.

For an admin user with a name other than `admin`, add the user to the `CNC#ALL-ACCESS` group.

```
ncs_cli -u admin
configure
set nacm groups group "CNC#ALL-ACCESS" user-name admin
commit dry-run
commit
```

For a non-admin user, create a NACM group that matches the Device Access Group. This example uses `RW-CW` as the user and `DAG-2` as the Device Access Group.

```
ncs_cli -u admin
configure
set nacm groups group "CNC#DAG-2" user-name RW-CW
commit dry-run
commit
```

Step 3 Generate the NACM rules in Crosswork and apply the rules to NSO.

In Crosswork, choose **Administration** > **Users and Roles** > **Users** > **Generate NACM Rules**. Apply the generated rules to NSO by using Commit Manager or by copying the XML to a file such as `sample-nacm.xml` and loading it with the merge operation.

```
ncs_cli -u admin
configure
load merge /home/nso/sample-nacm.xml
commit
```

Step 4 Add the standalone NSO provider in Crosswork.

See Add a standalone Cisco NSO provider.

Step 5 Install the required Cisco NSO function packs.

See the NSO function pack installation topics in this chapter.

Restrict sync-to access for the Crosswork NSO user

Use this task to create a restricted NSO user for Crosswork authentication when you do not want the Crosswork-authenticated user to execute `sync-to`.

Before you begin

- Log in to the NSO server Linux shell.
- Know the user name and password that you want Crosswork to use when it authenticates to NSO.

Procedure

Step 1 Open the NSO CLI without authentication.

Example:

```
ncs_cli -C -noaaa
```

Step 2 Create an NACM rule list that denies `sync-to` access for the restricted Crosswork user group.

This example uses `restrictedCNC` as the NACM group name.

Example:

```
config
nacm rule-list CNC
group restrictedCNC
rule restrict-syncto action deny
module-name tailf-ncs
path /ncs:devices/device/sync-to
exit
rule restrict-multi-syncto action deny
module-name tailf-ncs
path /ncs:devices/sync-to
exit
rule restrict-group-syncto action deny
module-name tailf-ncs
```

```
path /ncs:devices/device-group/sync-to
exit
rule any-access action permit
exit
cmdrule any-command action permit
commit dry-run
commit
```

Step 3 Create the Linux group and user account for Crosswork authentication.

This example uses `restrictedCNC` as the Linux group name and `CNCuser` as the user name.

Example:

```
sudo groupadd restrictedCNC
sudo useradd CNCuser
sudo usermod -a -G restrictedCNC CNCuser
sudo passwd CNCuser
```

Step 4 When prompted, enter the password for the Crosswork-authenticated NSO user.

Step 5 Use the restricted user account when you configure Crosswork to authenticate to NSO.

Crosswork authenticates to NSO with a restricted user account that cannot execute `sync-to`.

Add a standalone Cisco NSO provider

The Cisco NSO provider supplies network services, device configuration services, device management, and configuration maintenance services to Crosswork applications.

Attention Crosswork Network Controller scans NSO for device status changes only after an explicit NSO action. To add devices from NSO to Crosswork Network Controller, perform an NSO action for a device, or update and save the NSO provider policy details.

Before you begin

- Create a credential profile for the Cisco NSO provider.
- Confirm the Cisco NSO device configurations.
- Know the provider name, server IP address or fully qualified domain name (FQDN), protocol, port, Network Element Driver (NED) model, and NED version for the provider. You can find the Cisco NSO version by using the `version` command.
- Make sure that the users who need the NSO cross-launch feature do not have read-only permissions.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access**.

Step 2 Click **Add**.

Step 3 Enter the required Cisco NSO provider field values.

Table 1: Standalone NSO provider fields

Field	Value
Provider Name	Enter the provider name.
Credential Profile	Select the Cisco NSO credential profile.
Family	Select **NSO**.
Protocol	Select **HTTPS**, **SSH**, or both. To use **Backup NSO**, configure SSH connectivity.
Server Details	Enter the IP address or FQDN of the NSO server. For NSO high availability (HA), use the management virtual IP (VIP) address.
Port	For HTTPS, enter the port configured in `/etc/ncs/ncs.conf`. The default NSO HTTPS port is **8888**.
Model	Select the model prefix that matches the NED CLI used by Cisco NSO. • Valid values are **Cisco-IOS-XR**, **Cisco-NX-OS**, and **Cisco-IOS-XE**. • Add a model for each device type in the topology. • For telemetry, only **Cisco-IOS-XR** is supported.
Version	Enter the NED software version installed for the device model in NSO.
Timeout	Enter the connection timeout in seconds. The default is 30 seconds.

Step 4 Enter the standalone NSO provider properties.

Table 2: Standalone NSO provider properties

Property key	Value
forward	Set to **true**. This property is required for Crosswork Network Controller provisioning operations in the UI and for the northbound interface to NSO through the Crosswork application programming interface (API) gateway. **Note** The default value is **false**. For Crosswork-to-NSO device-addition workflows, set this property to **true** and configure the relevant provider policy attributes in **Edit policy details**.
nso_crosslaunch_url	Enter the URL for cross-launching standalone NSO in this format: `https://<NSO IP address/FQDN>:<port-number>`

Step 5 Click **Save**.

Step 6 If the default policy values do not match your environment, edit the NSO provider policy details.

Use policy details to control how Crosswork matches, adds, synchronizes, and manages devices between Crosswork Network Controller and NSO.

a. On the NSO provider, choose **Actions** > **Edit policy details**.

b. Edit the configuration fields to match your environment.

c. Click **Save**.

Note
Set **Onboard from** to **`TRUE`** when Crosswork Network Controller must add devices from NSO and the devices do not have an IP address match. The default value is **`FALSE`**.

Table 3: Editable NSO provider policy attributes

Attribute	Description
Match	Set to **`True`** to match Crosswork Network Controller devices with NSO devices based on IP address.
MatchRule	Enter an expression that defines the subset of devices to match.
Onboard To NSO	Set to **`True`** to add missing devices to NSO.
Onboard To Rule	Enter an expression that defines the subset of devices to add to NSO.
Onboard From	Set to **`True`** to add devices from NSO to Crosswork Network Controller when they are missing.
Onboard From Rule	Enter an expression that defines the subset of devices to add from NSO.
Sync From	Set to **`True`** to run sync-from on the NSO device after Crosswork adds the device.
Sync From Rule	Enter an expression that defines the subset of devices for sync-from.
Check Sync	Set to **`True`** to check the synchronization status of NSO devices.
Check Sync Rule	Enter an expression that defines the subset of devices for check-sync.
NED	Specify the Network Element Driver (NED) to use. By default, NSO uses the latest CLI NED.
Rule	Enter an expression that defines which devices use a specific NED.

Step 7 Confirm with your network administrator whether proxy forwarding must be configured in your network. If proxy forwarding is required for the Crosswork UI, configure proxy forwarding on the NSO server.

Add the proxy-forwarding settings in the `ncs.conf` file on the NSO server.

Replace the example subnet and mask values with the values for your Crosswork Network Controller environment. If you have multiple subnets, repeat the `<allowed-proxy-ip-prefix>` blocks for each subnet.

Use the following example to configure proxy-forwarding settings in `ncs.conf`.

```
<webui>
...
  <use-forwarded-client-ip>
    <proxy-headers>X-Forwarded-For</proxy-headers>
    <proxy-headers>X-REAl-IP</proxy-headers>
```

```
    <allowed-proxy-ip-prefix>10.195.72.0/24</allowed-proxy-ip-prefix>
    <allowed-proxy-ip-prefix>2001:0db8:85a3:0000:0000:8a2e:0370::/112</allowed-proxy-ip-prefix>
  </use-forwarded-client-ip>
...
</webui>
```

Configure Cisco NSO for Layered Service Architecture

Use this workflow when your Crosswork deployment uses Cisco NSO Layered Service Architecture (LSA).

An LSA deployment uses customer-facing service (CFS) and resource-facing service (RFS) NSO nodes. Crosswork identifies the NSO provider as CFS or RFS, and only one CFS is allowed.

Before you begin

- Install a compatible Cisco NSO version and set up NSO LSA.
- Create the Crosswork credential profiles that you will use for the CFS and RFS providers.
- Know the CFS and RFS provider names, IP addresses or fully qualified domain names (FQDNs), protocols, ports, Network Element Driver (NED) models, and NED versions.

Procedure

Step 1 On each NSO RFS node, enable local authentication in the `ncs.conf` file under the `<aaa>` section.

Example:

```
<local-authentication>
  <enabled>true</enabled>
</local-authentication>
```

If you are using the CFS node, skip this step.

Step 2 Restart NSO on each RFS node.

Example:

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

Step 3 Enable service-level NETCONF Access Control Model (NACM) on both the CFS and RFS nodes.

Example:

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

Step 4 Configure user association for LSA role-based authentication.

- If NSO is used exclusively with Crosswork, remove the `auth-group default` map. If there are non-Crosswork NSO users, keep the default map and create an `auth-group umap` entry for every Crosswork user.

- Define each Crosswork user under `aaa:aaa` as an authentication user on every RFS node. The username must match the username in Crosswork, but the password can differ.
- Add every Crosswork user as a `umap` entry under the device authentication group in the CFS so that the CFS can pass user requests to the RFS node as the corresponding user.

Step 5 Define a generic NACM group and NACM rule with all permissions on the CFS.

When you create a user in Crosswork, add that user to the `CNC#ALL-ACCESS` NACM group in CFS.

```
group "CNC#ALL-ACCESS" {
  user-name [ RW-CW admin rw-user ];
}
```

Copy the NACM rules from Crosswork and apply them to the CFS and RFS nodes.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <!-- NACM rules for NSO - CFS -->
  <rule-list>
    <name>CNC#ALL-ACCESS#rule-list</name>
    <group>CNC#ALL-ACCESS</group>
    <rule>
      <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
      <action>permit</action>
      <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
    </rule>
    <cmdrule xmlns="http://tail-f.com/yang/acm">
      <name>any-access</name>
      <action>permit</action>
    </cmdrule>
  </rule-list>
</nacm>
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <!-- NACM rules for NSO - RFS -->
  <rule-list>
    <name>CNC#ALL-ACCESS#rule-list</name>
    <group>CNC#ALL-ACCESS</group>
    <rule>
      <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
      <action>permit</action>
      <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
    </rule>
    <cmdrule xmlns="http://tail-f.com/yang/acm">
      <name>any-access</name>
      <action>permit</action>
    </cmdrule>
  </rule-list>
</nacm>
```

Step 6 Add the Device Access Groups and NACM rules on the RFS node.

Crosswork automatically creates Device Access Groups, so you do not need additional NSO steps for this task. Apply the generated NACM rules to NSO by using Commit Manager or by loading the XML file with the merge operation.

Step 7 Add the LSA NSO providers in Crosswork.

See Add Cisco NSO providers for Layered Service Architecture.

Step 8 If Geo-HA is set up and you encounter a 503 error, add the proxy settings to the `/etc/environment` file on the CFS node.

```
https_proxy="http://proxy.esl.cisco.com:80"
http_proxy="http://proxy.esl.cisco.com:80"
```

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,<az1 mgmt vip>,<az2
 mgmt vip>,<fqdn of CW geo-mgmt VIP>"
```

Source the file, and then reboot the CFS nodes for the proxy settings to take effect.

Step 9 Install the required Cisco NSO function packs.

See the NSO function pack installation topics in this chapter.

Add Cisco NSO providers for Layered Service Architecture

Use this task to add the CFS and RFS NSO providers that Crosswork uses in an LSA deployment.

Crosswork supports Cisco NSO LSA deployments that use multiple NSO providers. The CFS NSO contains the services, and the RFS NSO contains the devices. Crosswork identifies the NSO provider as CFS or RFS, and only one CFS is allowed.

Attention Crosswork Network Controller scans NSO for device status changes only after an explicit NSO action. To add devices from NSO to Crosswork Network Controller, perform an NSO action for a device, or update and save the NSO provider policy details.

Before you begin

- Configure the CFS and RFS NETCONF Access Control Model (NACM) settings.
- Enable LSA settings in Crosswork before you add an NSO LSA provider.
- Make sure that RFS node IP addresses configured on the CFS match the RFS node IP addresses shown in the Crosswork UI. If the IP addresses do not match, Crosswork reports that the LSA cluster is missing RFS providers.
- Create the credential profiles for the LSA NSO providers.
- Confirm the Cisco NSO device configurations.

Procedure

Step 1 If LSA is not enabled, enable LSA settings in Crosswork.

a. Choose **Administration** > **Settings** > **System settings** > **Layered service architecture**.

b. Select **Enable**.

c. Select the device distribution method: **Round Robin**, **Capacity**, or **User Defined**.

d. Click **Save**.

Note
After you save the LSA setting, you cannot disable LSA without first removing all NSO providers.

Step 2 Choose **Administration** > **Manage Provider Access**.

Step 3 Click **Add**.

Step 4 Enter the required Cisco NSO provider field values for the CFS or RFS provider.

Table 4: LSA NSO provider fields

Field	Value
Provider Name	Enter the provider name.
Credential Profile	Select the Cisco NSO credential profile for this provider.
Family	Select **NSO**.
Protocol	Select **HTTPS**, **SSH**, or both. To use **Backup NSO**, configure SSH connectivity.
Server Details	Enter the IP address or fully qualified domain name (FQDN) of the CFS or RFS server. For NSO high availability (HA), use the management virtual IP (VIP) address.
Port	For HTTPS, enter the port configured in `/etc/ncs/ncs.conf`. The default NSO HTTPS port is **8888**.
Model	Select the model prefix that matches the Network Element Driver (NED) CLI used by Cisco NSO. • Valid values are **Cisco-IOS-XR**, **Cisco-NX-OS**, and **Cisco-IOS-XE**. • Add a model for each device type in the topology. • For telemetry, only **Cisco-IOS-XR** is supported.
Version	Enter the NED software version installed for the device model in NSO.
Timeout	Enter the connection timeout in seconds. The default is 30 seconds.

Step 5 Enter the LSA NSO provider properties.

Table 5: LSA NSO provider properties

Property key	Value
forward	Set to **true**. This property is required for Crosswork Network Controller provisioning operations in the UI and for the northbound interface to NSO through the Crosswork application programming interface (API) gateway. **Note** For a CFS node, only the **forward** property key is used. The default value is **false**. For Crosswork-to-NSO device-addition workflows, set this property to **true** and configure the relevant provider policy attributes in **Edit policy details**.

Property key	Value

input_url_prefix	For an LSA provider, enter the RFS ID in this format, where x is the RFS node number:
	`/rfc-x`
	Example for RFS node 1:
	`input_url_prefix: /rfc-1`

Step 6 Click **Save**.

Step 7 If the default policy values do not match your environment, edit the NSO provider policy details.

Use policy details to control how Crosswork matches, adds, synchronizes, and manages devices between Crosswork Network Controller and NSO.

a. On the NSO provider, choose **Actions** > **Edit policy details**.

b. Edit the configuration fields to match your environment.

c. Click **Save**.

Note
Set **Onboard from** to **TRUE** when Crosswork Network Controller must add devices from NSO and the devices do not have an IP address match. The default value is **FALSE**.

Table 6: Editable NSO provider policy attributes

Attribute	Description
Match	Set to **True** to match Crosswork Network Controller devices with NSO devices based on IP address.
MatchRule	Enter an expression that defines the subset of devices to match.
Onboard To NSO	Set to **True** to add missing devices to NSO.
Onboard To Rule	Enter an expression that defines the subset of devices to add to NSO.
Onboard From	Set to **True** to add devices from NSO to Crosswork Network Controller when they are missing.
Onboard From Rule	Enter an expression that defines the subset of devices to add from NSO.
Sync From	Set to **True** to run sync-from on the NSO device after Crosswork adds the device.
Sync From Rule	Enter an expression that defines the subset of devices for sync-from.
Check Sync	Set to **True** to check the synchronization status of NSO devices.
Check Sync Rule	Enter an expression that defines the subset of devices for check-sync.
NED	Specify the Network Element Driver (NED) to use. By default, NSO uses the latest CLI NED.

Attribute	Description
Rule	Enter an expression that defines which devices use a specific NED.

Step 8 Repeat this task for each required CFS and RFS provider.

What to do next

Install the required NSO function packs.

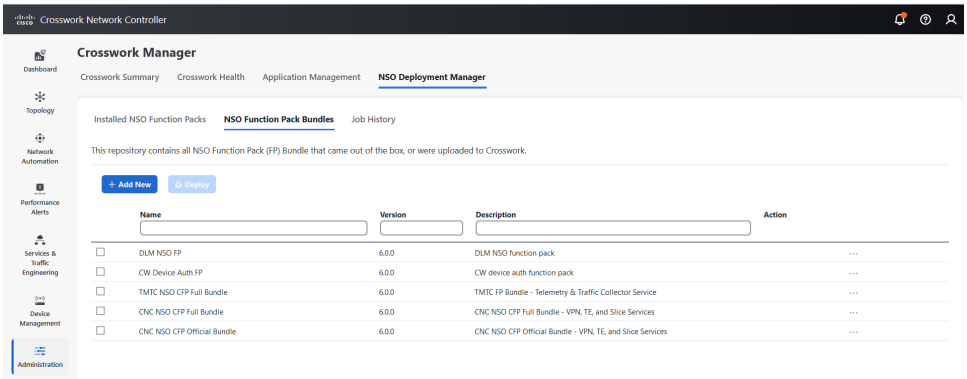
Install Cisco NSO Function Pack Bundles from Crosswork UI

In the Cisco NSO function pack bundles, the NSO function pack files are bundled as tar.gz files. To ensure interoperability with Crosswork, Cisco NSO requires the installation of the essential function packs.

In the Crosswork UI, the **NSO Deployment Manager** tab lets you manage the function pack bundles using the following tabs:

- **Installed NSO Function Packs**: Provides the list of NSO function packs deployed on the configured NSO server. See View NSO Function Pack Bundles, on page 12 for more information.
- **NSO Function Pack Bundles**: Allows you to add and deploy the function pack bundles. Use this tab, to view the artifacts in the function pack bundle, download, and delete the function pack bundles. See Manage NSO Function Pack Bundles, on page 13 for more information.
- **Job History**: The **Job History** tab displays a summary of the jobs, job ID, time when the job is started and completed, job description, and target. See View NSO Function Pack Job History, on page 19 for more information.

Figure 1: NSO Deployment Manager Window



View NSO Function Pack Bundles

Operators can retrieve a list of all of the function pack bundles installed on each available NSO server via the Crosswork UI or using the API.

Attention If any of the NSO service providers is unreachable, you cannot view the installed NSO function packs. An error "*Server is temporarily unavailable, try to relogin*" is displayed.

Follow the steps below to view the installed NSO function pack bundles through the UI.

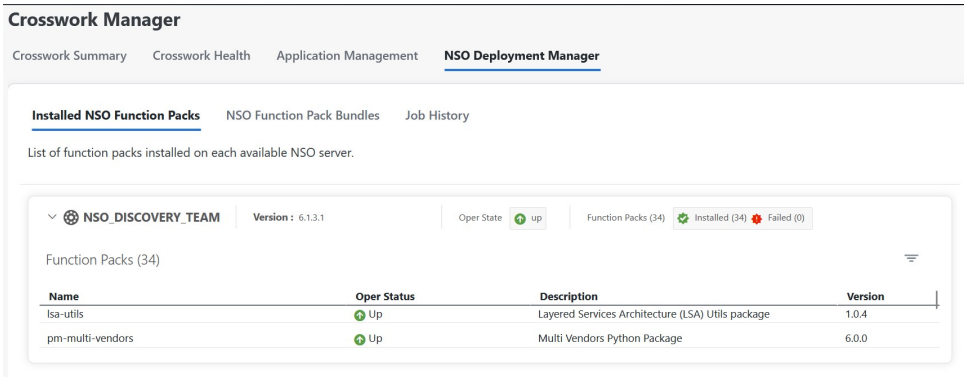
Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**, click the **NSO Deployment Manager** tab.

Step 2 Click the **Installed NSO Function Packs** tab.

Step 3 Select the NSO provider and expand the NSO server entry to view the list of function packs and their details (function pack name, operational state as **Up** or **Down**, description, and version).

Figure 2: Installed NSO Function Packs Window



Manage NSO Function Pack Bundles

You can add and deploy custom NSO function packs in addition to the function packs that are added by default to the Crosswork UI. The preinstalled bundles include the following packs:

Table 7: Default NSO Core Function Packs Bundles

Package Name	Contents
DLM NSO FP	Cisco NSO DLM Service Pack
Device Auth NSO FP	Cisco Crosswork Change Automation NSO Function Pack
TMTC NSO FP	Cisco NSO Telemetry Traffic Collector Function Pack
CNC NSO FPs Plus Sample FPs	Crosswork Network Controller NSO function packs for VPN, TE, and Slice services, with sample FPs included

Package Name	Contents
CNC NSO FPs	Crosswork Network Controller NSO function packs for VPN and TE services
Cisco NSO Traffic Engineering manager	Crosswork Network Controller NSO TE Manager for implicit service and transport provisioning.
CWM SOLUTION FPS **Note** Only available after deployment of Premier tier.	NSO Function Pack for Crosswork Workflow Manager Solutions

Before you begin

Ensure that these prerequisites are met:

- Java version 17.0.0 or higher is installed on the NSO server.
- Python version 3.11.0 or higher is installed on the NSO server.
- NSO is configured to allow 64,000 openFileDescriptors.

Procedure

Step 1 Ensure that your NSO setup meets all of the prerequisites.

Check the python and java versions using the `--version` command.

```
python --version

Python 3.11.0

java --version

openjdk 17.0.9 2023-10-17
OpenJDK Runtime Environment (build 17.0.9+9-Ubuntu-120.04)
OpenJDK 64-Bit Server VM (build 17.0.9+9-Ubuntu-120.04, mixed mode, sharing)
```

To verify or configure the required file descriptor limits on the NSO server, check the `/etc/security/limits.conf` file. If the required values are not already configured, add these lines before the commented line #End of file:

```
$ grep hard /etc/security/limits.conf
$ grep soft /etc/security/limits.conf
* soft nproc 65535
* hard nproc 65535
* soft nofile 65535
* hard nofile 65535
* soft memlock 65535
* hard memlock 65535
```

Step 2 From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.

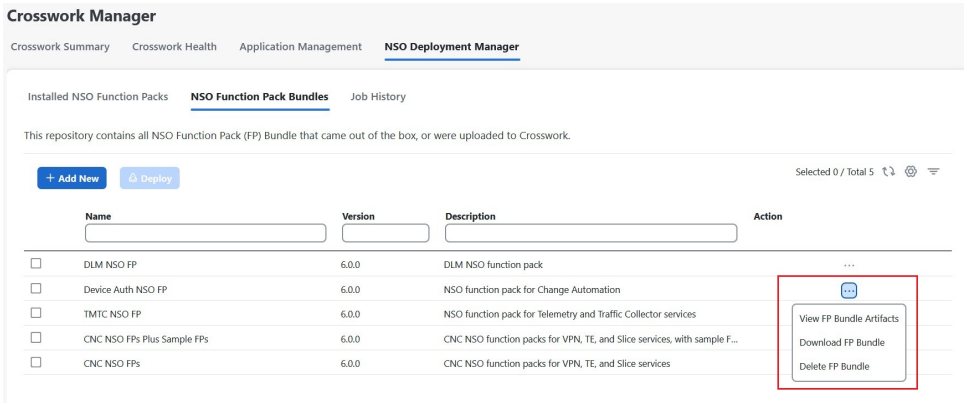
Step 3 Click the **NSO Function Pack Bundles** tab.

All the installed NSO function pack bundles get displayed with the bundle name, version, and description information.

To manage the bundles, select one or more bundles and click the **Action** menu to perform the following:

- **View FP Bundle Artifacts**: View the hierarchy of the artifacts that are bundled in the selected package.
- **Download FP Bundle**: Download the function pack bundle.
- **Delete FP Bundle**: Delete the function pack bundle.

Figure 3: Action Menu



Step 4 Click **Add New** to install the new function pack bundle. The **Add New NSO Function Pack Bundle** page is displayed.

Note
The **Add New** button is disabled when Crosswork is in maintenance mode.

Step 5 In the **Add New NSO Function Pack Bundle** page, enter the following:

- **Host Name/IP address**: Enter the IP address and subnet mask of the Cisco NSO server.
- **Port**: For HTTPS, enter the port that corresponds with what is configured on the NSO VM in etc/ncs/ncs.conf to access NSO using HTTPS. NSO uses 8888 as the default port.
- **User Name**: The username used to log in to the NSO server.
- **Password**: The password credentials to authenticate into the NSO server.
- **Server Path/Location**: The server path of the NSO server.

Step 6 Click **Test SSH Connectivity** again to validate SSH-based connectivity. If the connection is successful, a confirmation message indicating that the NSO bundle upload is in-progress appears. Click **View Progress in Job History** to view the upload status.

Step 7 Click **Add**.

Step 8 Check the **Job History** to monitor the addition of the package to Crosswork. Once the package has been added, the next step is to deploy the function pack.

What to do next

After the function pack is added, deploy the function pack on NSO. See Deploy NSO function packs bundles, on page 16.

Deploy NSO function packs bundles

This topic explains the process to deploy the NSO function pack bundles.

The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.

Attention NSO function packs cannot be deployed when Crosswork is in maintenance mode.

Before you begin

- Ensure that the NSO function pack bundle is uploaded to the Crosswork UI. See Manage NSO Function Pack Bundles, on page 13 for more information.
- If you plan to deploy the function pack bundle in an HA environment, you must have the primary and secondary server details readily available.
- If your primary and secondary NSO servers and Crosswork servers are in different subnets, you must configure either an IP static route (**Administration** > **Settings** > **Static Routes**) or an IP rule policy (run `ip rule add from all to 10.19.0.4 lookup cw_data` on the Crosswork server) to enable connectivity between the servers.

Procedure

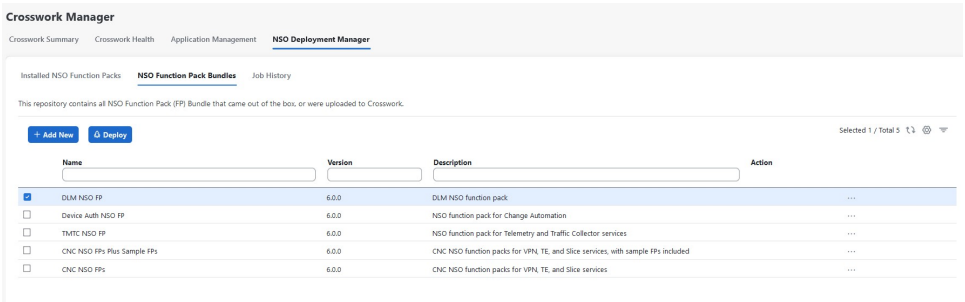
Step 1 From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.

Step 2 Click the **NSO Function Pack Bundles** tab.

Step 3 Select the NSO function pack bundle and click **Deploy**.

Note
You can only select up to 3 Function Packs to be installed at a time. To install more, install the 3 function packs first and then repeat this process until you have installed all the Function Packs you will use.

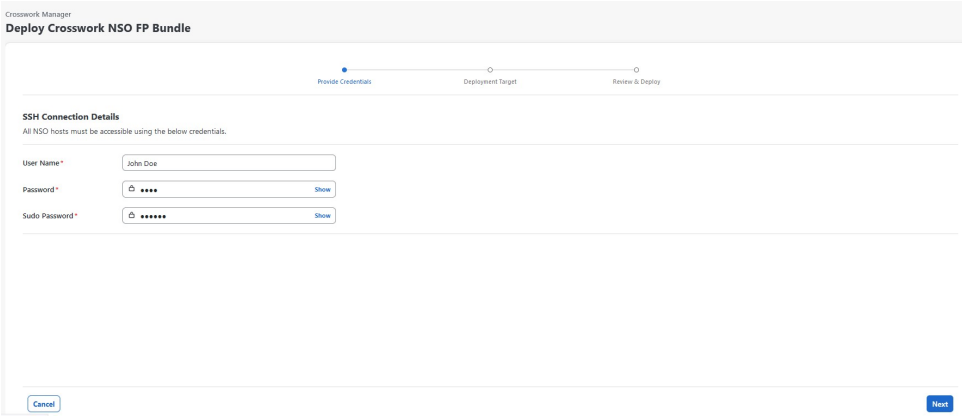
Figure 4: NSO Function Pack Bundles Window



Step 4 In the **Deploy Crosswork NSO FP Bundle** page, enter the following SSH connection details:

- **User Name**: The SSH username for server access.
- **Password**: The SSH password for server access.
- **Sudo Password**: The SSH sudo password.

Figure 5: SSH Connection Details Page

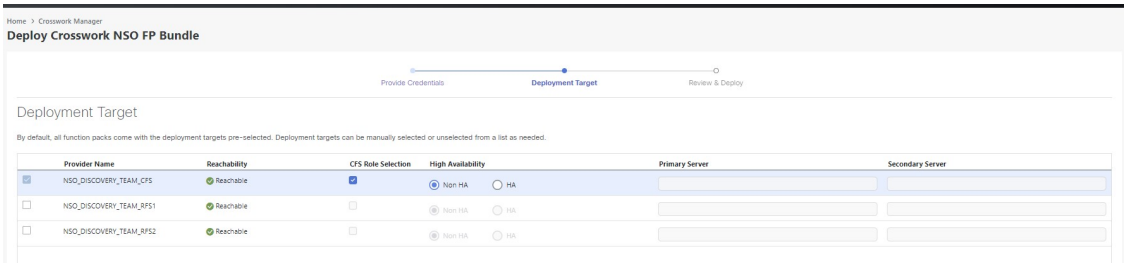


Step 5 Click **Next**.

Step 6 In the **Deployment Target** section, review the target details:

- **Provider Name**: Displays the name of the provider.
- **Reachability**: Displays the reachability status of the provider.
- **CFS Role Selection**: This column appears when a role is not assigned to a provider. Select the check box that corresponds to the provider row to assign the customer-facing service (CFS) role. The resource-facing service (RFS) role is automatically assigned to the other providers. For more information about CFS, RFS, and Cisco NSO Layered Service Architecture (LSA) deployment concepts, see the *Prepare Infrastructure for Device Management* chapter in the *Cisco Crosswork Network Controller 7.2.x Administration Guide*.
- **High Availability**: Depending on your deployment preferences for the function packs bundle on an NSO node, select either non-HA or HA. If you have selected HA, enter the server details in the **Primary Server** and **Secondary Server** fields.

Figure 6: Deployment Target Page

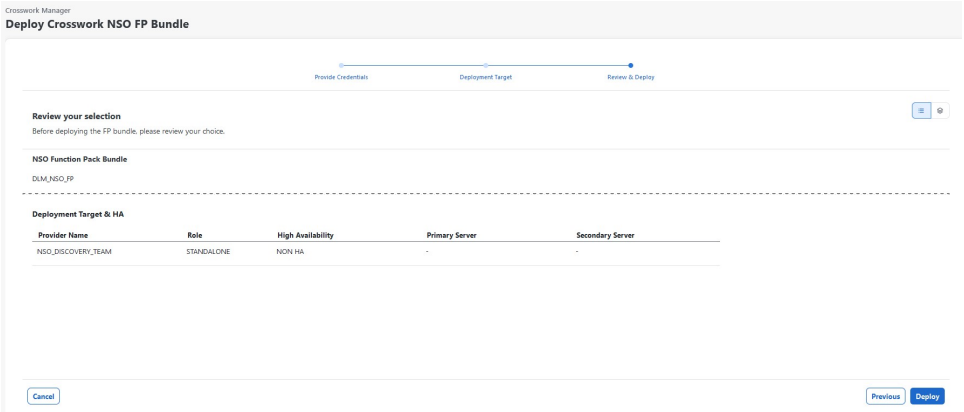


Step 7 Click **Next**.

Step 8 In the **Review & Deploy** page, review the NSO bundle and deployment target details that you have configured. If you want to modify your selection, click **Previous** to view the earlier pages and modify it as required.

Note
If the provider is deployed on a standalone NSO node, the role is displayed as STANDALONE.

Figure 7: Review Selection Page



Step 9 Click **Deploy**.

Step 10 Check the **Job History** to monitor the installation.

Step 11 Repeat the process for any additional Function Packs that you need to install.

Troubleshoot the NSO Function Pack Installation

The following table lists common problems that might be experienced while installing or deploying a Cisco NSO function pack.

Table 8: Troubleshooting the Function Pack Installation Issues

Issue	Action
The function pack deployment failed with the following error: `Failed to open SSH connection to host coffee-nso1.cisco.com`	In an HA configuration, the NSO engine assumes that the NSO primary and secondary servers, and the Crosswork server reside in the same subnet. If the servers have different subnets, you must configure an IP route or an IP rule policy to ensure connectivity between the servers. When the routes are not configured, the engine cannot locate the subnet, and the function pack deployment fails. **Note** Static routes can only be configured when ZTP application is installed. Use one of the following steps to resolve the issue: • To configure the static routes, from the main menu, select **Administration** > **Settings** > **Static Routes**. Click the + icon, enter the destination subnet IP address and mask (in slash notation), then click **Add**. • To configure the IP rule, log in to the Crosswork server and use the following command: `ip rule add from all to 10.19.0.4 lookup cw_data`

View NSO Function Pack Job History

The **Job History** tab shows detailed information of when jobs were started and ended, job ID, status, and other vital information.

Follow the steps below to view the details of the jobs.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**, click the **NSO Deployment Manager** tab.

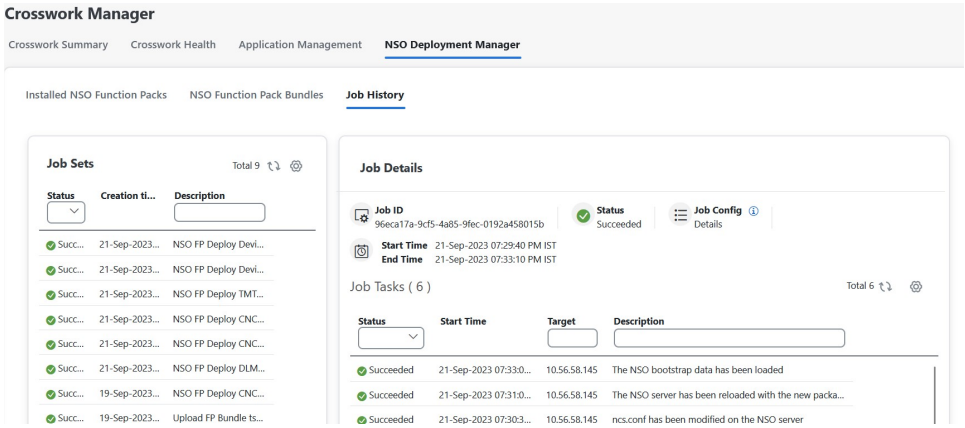
Step 2 Click the **Job History** tab.

In the **Job History** tab, the **Job Sets** pane displays the state of the job, job ID, and the job description. You can show or hide the columns based on the job creation time, status, and description.

Step 3 In the **Job Sets** pane, select the job sets to view the associated job information in the **Job Details** pane. You can view the summary of the job tasks based on job task ID, task status, the task start and end time, and description.

To view the job configuration information in JSON format, click the icon next to **Job Config**. A config window opens that lets you view the configuration in *View mode*.

Figure 8: Job History Window



Install NSO function packs manually

If you need to install or configure the NSO function packs manually, follow the instructions in these links:

- *Cisco NSO Transport SDN Function Pack Bundle 7.2.x User Guide*
- *Cisco NSO Transport SDN Function Pack Bundle 7.2.x Installation Guide*
- *Cisco Network Services Orchestrator DLM Service Pack 7.2.x Installation Guide*
- *Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 7.2.x Installation Guide*
- *Cisco Crosswork Change Automation NSO Function Pack 7.2.x Installation Guide*
- *Cisco NSO Auto Discovery Installation and User Guide 7.2.x*

Configure JSON Web Token authentication for NSO

Use this task after the required Cisco NSO function packs are installed and before you validate Crosswork-to-NSO communication. The Crosswork certificate must be available on the NSO VM before you configure NSO to use the JWT authentication package.

Export the certificate from the browser and workstation that you use to access Crosswork. After you export the certificate, copy the certificate file to the NSO VM and complete the NSO-side configuration.

Warning Do not perform this task until the required Cisco NSO function pack bundle is installed. The JWT authentication package is installed with the function pack bundle.

Procedure

Step 1 In the browser that you use to access Crosswork, open the Crosswork website.

Step 2 Click the padlock icon in the address bar, and then choose **Certificate is not Valid** > **View Certificate**.

Step 3 In the **Certificate Viewer** window, click the **Details** tab.

Step 4 Under **Certificate Hierarchy**, click **Crosswork**.

Step 5 Click **Export**, choose a file name and location, and save the certificate as a Base64-encoded ASCII single certificate.

Use the `.pem` extension. For example, save the file as `crosswork.pem`.

Note
If you cannot save the file in `.pem` format, save it as a `.cer` file and use that file path in the bootstrap configuration.

Step 6 Copy the certificate file to the NSO VM.

Note
Make sure that the pem-key-path value and certificate file name are the same on the primary and secondary host.

Step 7 On the NSO VM, open the `ncs.conf` file in the NSO directory, and add the JWT package authentication configuration under the `<aaa>` section.

Example:

```
<aaa>
  <package-authentication>
    <enabled>true</enabled>
    <packages>
      <package>cisco-cfp-jwt-auth</package>
    </packages>
  </package-authentication>
</aaa>
```

Step 8 Restart NCS for the `ncs.conf` configuration to take effect.

Example:

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

Step 9 Configure the bootstrap authentication package by using `ncs_cli`.

Log in to `ncs_cli`, enter configuration mode, and run these commands:

```
set jwt-auth cnc-host <Crosswork IP>
set jwt-auth port 30603
set jwt-auth pem-key-path /home/nso/crosswork.pem
commit dry-run
commit
```