



# Integrate Cisco NSO

---

This chapter contains the following topics:

- [NSO Integration Workflow](#), on page 1
- [Install Cisco NSO Function Pack Bundles from Crosswork UI](#), on page 2
- [Install Cisco NSO Function Packs Manually](#), on page 11
- [Add Cisco NSO Providers](#), on page 11
- [\(Optional\) Set up Cisco NSO Layered Service Architecture](#), on page 13

## NSO Integration Workflow

This section explains the steps in integrating Cisco NSO with Crosswork Network Controller.

### 1. Install the compatible version of Cisco NSO

Ensure that you have installed the compatible version of Cisco NSO:

- If you are a VMware user, follow the instructions in [NSO documentation](#).
- If you are a AWS EC2 user, follow the instructions in [Install Cisco NSO on Amazon EC2](#).

Additionally, for Cisco NSO LSA setup, see [\(Optional\) Set up Cisco NSO Layered Service Architecture](#), on page 13.

See the *Compatibility Information* section in the *Crosswork Network Controller 6.0 Release Notes* for information on the compatible versions of NSO/NED.

### 2. Install the mandatory NSO core function packs

Depending on the Cisco Crosswork application or solution that you are using, there are mandatory Core Function Packs (CFPs) that must be installed on Cisco NSO to make the products compatible.

The NSO core function packs are bundled in [cisco.com](https://www.cisco.com) as follows:

Table 1: NSO Core Function Packs

Package Name	Contents
Cisco Crosswork Network Controller Essential Function Pack <b>File name:</b> <i>signed-cw-cnc-essential-fp-6.0.0.tar.gz</i>	<ul style="list-style-type: none"> <li>• <i>Cisco NSO Transport SDN Function Pack Bundle</i></li> <li>• <i>Cisco NSO DLM Service Pack</i></li> <li>• <i>Cisco NSO Telemetry Traffic Collector Function Pack</i></li> </ul>
Cisco Crosswork Change Automation Function Pack <b>File name:</b> <i>nca-6.0.0-nso-6.1.4.signed.bin</i>	<ul style="list-style-type: none"> <li>• <i>Cisco Crosswork Change Automation NSO Function Pack</i></li> </ul>

You can install the CFPs using either of the following methods:

- [Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 2](#) (Recommended)
- [Install Cisco NSO Function Packs Manually, on page 11](#)



**Note** The Cisco Crosswork Network Controller Function Pack SDK Application (*cw-na-platform-6.0.0-signed-tdn-sdk.tar.gz*) is also available for download on [cisco.com](http://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.

### 3. Add the NSO provider and verify connectivity

Follow the instructions in [Add Cisco NSO Providers, on page 11](#).

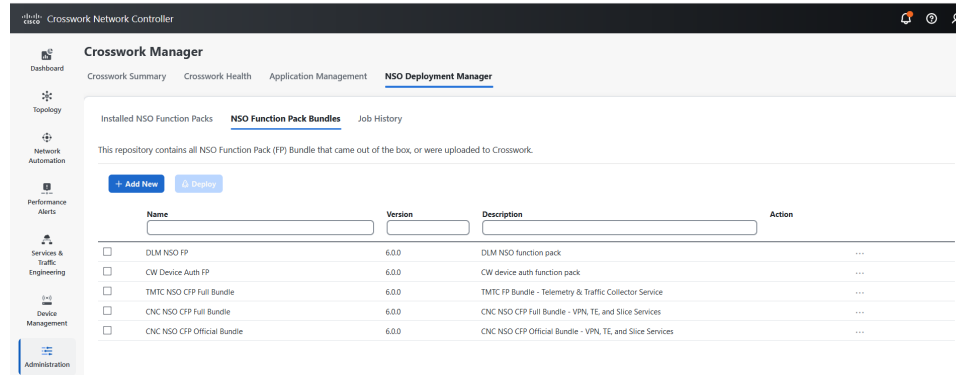
## Install Cisco NSO Function Pack Bundles from Crosswork UI

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 3](#) 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 4](#) for more information.
- **Job History:** Displays the status of the function pack jobs since they were submitted. 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 10](#) for more information.

Figure 1: NSO Deployment Manager Window



## View NSO Function Pack Bundles

The Crosswork UI provides the list of function pack bundles installed on each available NSO server. The bundles include the default and the custom functions pack bundles that you have uploaded to the Crosswork UI.

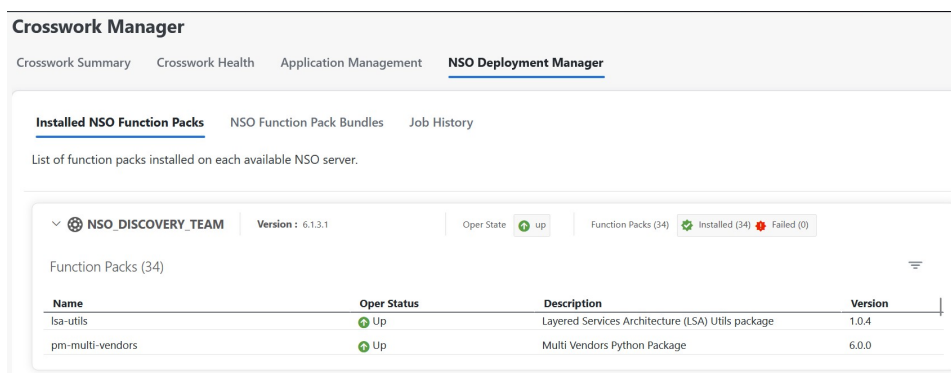


**Attention** If any of the NSO service providers is unreachable, you cannot view the installed NSO function packs. An error "Server is temporarily unavailable, try to relogin" is displayed.

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

- 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** Expand the bundles to view the number of function packs within each bundle, the 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 2: 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. It also contains the sample function packs.
CNC NSO FPs	Crosswork Network Controller NSO function packs for VPN, TE, and Slice services.

### Before you begin

Each function pack bundle includes a metadata.yaml file detailing the prerequisites for installing the bundle on NSO. The following is a comprehensive list of the prerequisites for the supplied function packs:

- Java version 11.0.0
- Python version 3.8.0
- NSO configured to allow 64,000 openFileDescriptors

Follow the steps below to manage the function pack bundles.

---

**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 3.8.10
```

```
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)
```

**Step 2** Click **Test SSH Connectivity** to validate if Crosswork is able to establish an SSH-based connection. The connectivity test might take some time and must not be interrupted.

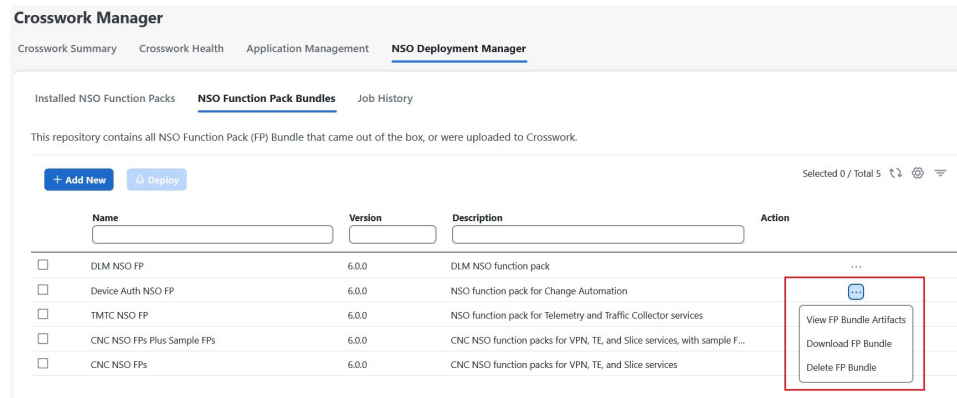
**Step 3** From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.

**Step 4** 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 5** Click **Add New** to install the new function pack bundle.

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.

Figure 4: Add New NSO Function Packs Bundle Window

Crosswork Manager

### Add New Nso Function Pack Bundle


**Upload NSO Function Pack Bundle**  
Use the Secure Copy(SCP) protocol to upload the file(.tar.gz).

Host Name / Ip Address\*

Port\*

User Name\*

Password\*  [Show](#) [Test SSH Connectivity](#)

Server Path/Location\*  

[+ Add Another](#)

[Add](#) [Cancel](#)

**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**.

#### What to do next

After the function pack is added, deploy the function pack on NSO. See [Deploy NSO Function Pack Bundles, on page 6](#).

## Deploy NSO Function Pack Bundles

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



**Note** 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.


### Before you begin

- Ensure that the NSO function pack bundle is uploaded to the Crosswork UI. See [Manage NSO Function Pack Bundles, on page 4](#) 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 or an IP rule policy to enable connectivity between the servers.



**Note** Static routes can only be configured when ZTP application is installed.

#### • Static routes configuration

From the Crosswork UI's main menu, select **Administration > Settings > Static Routes**. Click the  icon, enter the destination subnet IP address and mask (in slash notation), then click **Add**.

#### • IP rule configuration

Log in to the Crosswork server and execute the following command:

```
ip rule add from all to 10.19.0.4 lookup cw_data
```

- 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 5: NSO Function Pack Bundles Window**

Name	Version	Description	Action
<input checked="" type="checkbox"/> DLM NSO FP	6.0.0	DLM NSO function pack	...
<input type="checkbox"/> Device Auth NSO FP	6.0.0	NSO function pack for Change Automation	...
<input type="checkbox"/> TMTC NSO FP	6.0.0	NSO function pack for Telemetry and Traffic Collector services	...
<input type="checkbox"/> CNC NSO FPs Plus Sample FPs	6.0.0	CNC NSO function packs for VPN, TE, and Slice services, with sample FPs included	...
<input type="checkbox"/> CNC NSO FPs	6.0.0	CNC NSO function packs for VPN, TE, and Slice services	...

**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 6: 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 6.0 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 7: Deployment Target Page

Provider Name	Reachability	CFS Role Selection	High Availability	Primary Server	Secondary Server
<input checked="" type="checkbox"/> NSO_DISCOVERY_TEAM_CFS	<input checked="" type="checkbox"/> Reachable	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Non-HA <input type="radio"/> HA		
<input type="checkbox"/> NSO_DISCOVERY_TEAM_RFS1	<input checked="" type="checkbox"/> Reachable	<input type="checkbox"/>	<input type="radio"/> Non-HA <input type="radio"/> HA		
<input type="checkbox"/> NSO_DISCOVERY_TEAM_RFS2	<input checked="" type="checkbox"/> Reachable	<input type="checkbox"/>	<input type="radio"/> Non-HA <input type="radio"/> HA		

**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 8: Review Selection Page**

Crosswork Manager  
Deploy Crosswork NSO FP Bundle

Provide Credentials    Deployment Target    Review & Deploy

**Review your selection**  
Before deploying the FP bundle, please review your choice.

**NSO Function Pack Bundle**  
DLM\_NS0\_FP

**Deployment Target & HA**

Provider Name	Role	High Availability	Primary Server	Secondary Server
NSO_DISCOVERY_TEAM	STANDALONE	NON HA	-	-

Cancel    Previous    Deploy


**Step 9** Click **Deploy**.

**Step 10** 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 3: Troubleshooting the Function Pack Installation Issues

Issue	Action
<p>The function pack deployment failed with the following error:</p> <pre>Failed to open SSH connection to host coffee-ns01.cisco.com</pre>	<p>In an HA configuration, the NSO engine assumes that the NSO primary and secondary servers, and the Crosswork server reside in the same subnet.</p> <p>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.</p> <p><b>Note</b> Static routes can only be configured when ZTP application is installed.</p> <p>Use one of the following steps to resolve the issue:</p> <ul style="list-style-type: none"> <li>To configure the static routes, from the main menu, select <b>Administration &gt; Settings &gt; Static Routes</b>. Click the  icon, enter the destination subnet IP address and mask (in slash notation), then click <b>Add</b>.</li> <li>To configure the IP rule, log in to the Crosswork server and use the following command: <pre>ip rule add from all to 10.19.0.4 lookup cw_data</pre> </li> </ul>

## View NSO Function Pack Job History

The **Job History** tab shows the historical 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.

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

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

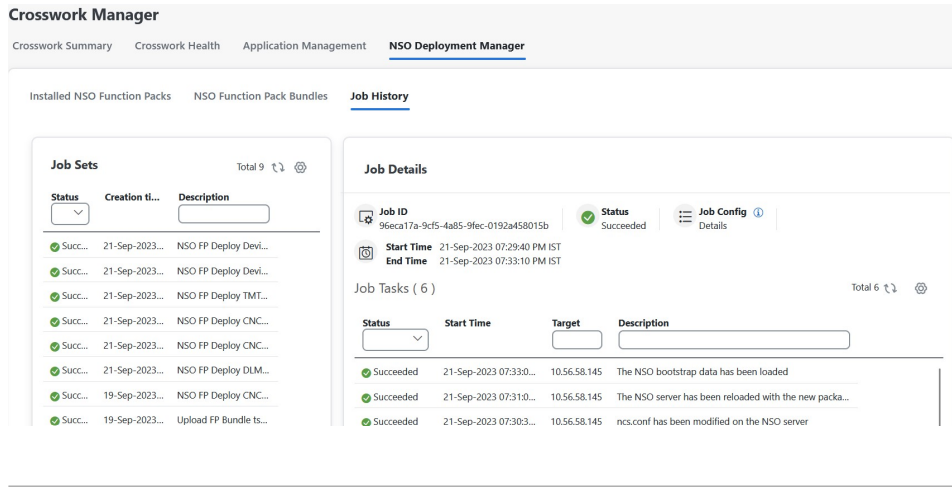
In the **Job History** tab, the **Job Sets** pane displays the state of the job, job ID, and the job description. You can show or hide the columns based on the job creation time, status, and description.

**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 the following modes:

- View Mode
- Text Mode

Figure 9: Job History Window



## Install Cisco NSO Function Packs Manually

If you need to install individual function packs manually, follow the relevant procedure from the below table:

**Table 4: List of Mandatory Function Packs**

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Essentials OR Crosswork Network Controller Advantage	<ul style="list-style-type: none"> <li><a href="#">Cisco NSO Transport SDN Function Pack Bundle 6.0.0 User Guide</a></li> <li><a href="#">Cisco NSO Transport SDN Function Pack Bundle 6.0.0 Installation Guide</a></li> <li><a href="#">Cisco Network Services Orchestrator DLM Service Pack 6.0.0 Installation Guide</a></li> <li><a href="#">Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 6.0.0 Installation Guide</a></li> <li><a href="#">Cisco Crosswork Change Automation NSO Function Pack 6.0.0 Installation Guide</a></li> </ul>
Crosswork Optimization Engine (Standalone)	<ul style="list-style-type: none"> <li><a href="#">Cisco Network Services Orchestrator DLM Service Pack 6.0.0 Installation Guide</a></li> <li><a href="#">Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 6.0.0 Installation Guide</a></li> </ul>

## Add Cisco NSO Providers

The Cisco Network Services Orchestrator (Cisco NSO) provider supplies the following functionality:

- Network services and device configuration services to Cisco Crosswork applications.
- Device management and configuration maintenance services.




---

**Note** Crosswork supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.

---

### Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider.
- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO version using the `version` command, as shown in the below example:

```
admin@ncs# show ncs-state version
ncs-state version 6.1.4
```

- Know the Cisco NSO NED device models and driver versions used in your topology.
- Know the Cisco NSO server IP address and hostname. When NSO is configured with HA, the IP address would be management VIP address.
- Confirm Cisco NSO device configurations.

Follow the steps below to add a Cisco NSO provider through the UI. Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Crosswork.

---

**Step 1** From the main menu, choose **Administration > Manage Provider Access**.

**Step 2** Click .

**Step 3** Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name:** Enter a name for the provider.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO**.
- Under Connection Type(s), **Protocol:** Select the protocol that Cisco Crosswork applications will use to connect to the provider. **HTTPS** is usually preferred.
- **IP Address/Subnet Mask:** Enter the IP address and subnet mask of the Cisco NSO server.

**Important** When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

- **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 default port.
- **Model:** Select the model (**Cisco-IOS-XR**, **Cisco-NX-OS**, or **Cisco-IOS-XE**) from the drop-down list and enter its associated NED driver version. Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.
- **Version:** Enter the NED software version installed for the device model in NSO.


b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

**Step 4** Under Provider Properties, enter a **Property Key** of **forward** and a **Property Value** of **true**. This property is necessary when using the Cisco Crosswork Network Controller solution to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway.

**Note** Cisco Crosswork provides the option to cross launch the NSO application from the Crosswork UI (this feature is not available for user roles with read-only permissions). To enable the cross launch feature, add Cisco NSO as a provider with one of the following settings:

- The **Property Key** `nso_crosslaunch_url` has a valid URL entered in the **Property Key** field.
- Protocol is **HTTP** or **HTTPS**, and the provider is reachable.

If any of the above settings are present, the cross launch icon (  ) is displayed in the **Provider Name** column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.

**Step 5** When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

**Step 6** In the Providers window, select the NSO provider you created and click **Actions > Edit Policy Details**.

The **Edit Policy Details** window for the selected NSO provider is displayed.

**Step 7** Edit the configuration fields to match the requirements of your environment. Click **Save** to save your changes.

---

### What to do next

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2](#)

## (Optional) Set up Cisco NSO Layered Service Architecture

This section is applicable only when you have opted for Cisco NSO Layered Service Architecture (LSA) deployment.

Cisco NSO LSA allows you to add arbitrarily many device nodes for improved memory and provisioning throughput. Large service providers or enterprises use Cisco NSO to manage services for millions of subscribers or users, ranging over several hundred thousand managed devices. To achieve this, you can design your services in the layered fashion called LSA.

To position Cisco Crosswork Network Controller for large customers, the solution is made compatible with the existing Cisco NSO LSA architecture.

Follow these steps to decide when to use Cisco NSO LSA:

1. Check if the deployment is stand-alone or Cisco NSO LSA.
2. If the deployment is stand-alone, check the maximum memory that may be utilised. If the maximum memory that may be utilised is more than the current memory state, Cisco NSO LSA needs to be deployed.



---

**Note** Migration from stand-alone deployment to Cisco NSO LSA deployment is not currently supported.

---

To get a detailed information on Cisco NSO LSA and to set up Cisco NSO LSA, see [NSO Layered Service Architecture](#).