



Cisco Crosswork Change Automation NSO Function Pack Installation Guide

Version 4.4.0

Contents

Introduction	3
Installing and Configuring	4
Installing Function Pack	4
Creating a Special Access User in Cisco NSO	4
Adding usermap (umap) to Cisco NSO authgroup	6
Configuring DLM in Cisco Crosswork	8
Create ca_device_auth_nso Credential Profile.....	8
Add DLM Provider Property	9
Troubleshooting.....	11

Introduction

This document describes how to download, install, and configure the Cisco Crosswork Change Automation (CA) function pack on Cisco Network Services Orchestrator (NSO). Additionally, the document describes the configuration required for Crosswork Change Automation in Cisco Crosswork.

Purpose

This guide describes:

- Installing the **cw-na-fp-ca-4.4.0-nso-5.7.6.tar.gz** function pack on Cisco NSO 5.7.6 and the associated configurations for the function pack on Cisco NSO.
- The **authgroup** configurations for creating a unique usermap (**umap**) for Change Automation.
- DLM configurations, and the Change Automation application settings required in Cisco Crosswork 4.4.0.

Pre-requisites

The list below shows the minimum versions of the Cisco NSO and Cisco Crosswork with which the Crosswork Change Automation function pack v4.4.0 is compatible.

- Cisco NSO: v5.7.6 system install
- Cisco Crosswork: v4.4.0

Installing and Configuring

The sections below show how to install the **cw-device-auth** function pack on system install Cisco NSO 5.7.6 or higher.

Installing Function Pack

1. Download the **cw-device-auth** v4.4.0 from the [repository](#) to your Cisco NSO.
2. Copy the downloaded tar.gz archive of the function pack to your package repository.

Note: The package directory can be different based on the selected settings at the time of installation. For most system-installed Cisco NSO, the package directory is located at “/var/opt/ncs/packages” by default. Check the ncs.conf on your installation to find your package directory.

3. Launch NCS CLI and run the following commands:

```
admin@nsol:~$ ncs_cli -C -u admin
admin connected from 2003:10:11::50 using ssh on nsol
admin@ncs# packages reload
```

4. Verify that the package has been successfully installed once the reload is complete.

```
admin@ncs# show packages package cw-device-auth
packages package cw-device-auth
package-version 4.4.0
description      "Crosswork device authorization actions pack"
ncs-min-version [ 5.7.6]
python-package  vm-name cw-device-auth
directory        /var/opt/ncs/state/packages-in-use/1/cw-device-auth
component action
application python-class-name cw_device_auth.action.App
application start-phase phase2
oper-status up
```

Creating a Special Access User in Cisco NSO

Cisco Crosswork Change Automation uses a special access user to connect to Cisco NSO for all configuration changes. This means that you cannot use the same user as DLM or collection services to access Cisco NSO. This section discusses the pre-requisites required for user creation.

Note: The steps below assume that Cisco NSO is running on a ubuntu VM. If your Cisco NSO installation is running on a different operating system, please modify the steps accordingly.

1. Create a new sudo user on your ubuntu VM. Example [here](#). The steps below show how to create user “**cwuser**” on your ubuntu VM. This new username can be anything of your choice.

```
root@nso:/home/admin# adduser cwuser
Adding user `cwuser' ...
Adding new group `cwuser' (1004) ...
```

```

Adding new user `cwuser' (1002) with group `cwuser' ...
Creating home directory `/home/cwuser' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for cwuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@nso:/home/admin# usermod -aG sudo cwuser
root@nso:/home/admin# usermod -a -G ncsadmin cwuser

```

2. Ensure that the new user that you created, has HTTP & HTTPS access to the Cisco NSO server. This can be done by using a simple RESTCONF API as shown below.

```

curl -u <USERNAME>:<PASSWORD> --location --request
GET 'https://<IP>:8888/restconf/data/taillf-ncs:packages/package=cw-device-auth' \
--header 'Accept: application/yang-data+json' \
--header 'Content-Type: application/yang-data+json' \
--data-raw ''

```

Upon calling the curl command above, you should receive a response as seen below. Any other response would indicate that one more setting before this did not work.

```

{
  "taillf-ncs:package": [
    {
      "name": "cw-device-auth",
      "package-version": "1.0.0",
      "description": "Crosswork device authorization actions pack",
      "ncs-min-version": ["5.4.0.2"],
      "python-package": {
        "vm-name": "cw-device-auth"
      },
      "directory": "/var/opt/ncs/state/packages-in-use/1/cw-device-auth",
      "component": [
        {
          "name": "action",
          "application": {
            "python-class-name": "cw_device_auth.action.App",
            "start-phase": "phase2"
          }
        }
      ]
    }
  ]
}

```

```

    ],
    "oper-status": {
      "up": [null]
    }
  }
]
}

```

Adding usermap (umap) to Cisco NSO authgroup

Cisco NSO allows users to define authgroups for specifying credential for southbound device access. An authgroup will always contain a default-map. A default-map contains the default login credentials for the devices. Additionally, a usermap (umap) can be defined in the authgroup for overriding the default credentials from default-map.

The Crosswork Change Automation “override credentials passthrough” feature uses this umap. To use Crosswork Change Automation, a umap configuration needs to be created in the authgroup for the devices.

For example, consider you have a device “**xrv9k-1**” enrolled in Cisco NSO. This device uses the authgroup, “**crosswork**”.

```

cwuser@ncs# show running-config devices device xrv9k-1 authgroup
devices device xrv9k-1
  authgroup crosswork
!

```

And the configuration of the authgroup “**crosswork**” is as follows:

```

cwuser@ncs# show running-config devices authgroups group crosswork
devices authgroups group crosswork
  default-map remote-name admin
  default-map remote-password $9$/KV4JLy6+sytQ6DYgHUzZZKfStK0G9G9BOuJMraQw7A=
!
!

```

Add a **umap** for the new user you have created (**cwuser** in this example). This can be done as follows:

```

cwuser@ncs(config)# devices authgroups group crosswork umap cwuser callback-node /cw-creds-
get action-name get
cwuser@ncs(config-umap-cwuser)# commit dry-run
cli {
  local-node {
    data devices {
      authgroups {
        group crosswork {
          +          umap cwuser {
          +            callback-node /cw-creds-get;
          +            action-name get;
          +          }
        }
      }
    }
  }
}

```


Configuring DLM in Cisco Crosswork

After installing and configuring the function pack in Cisco NSO, you need to setup the configuration in DLM in Cisco Crosswork. These configuration settings will allow Change automation to access Cisco NSO via the newly created user and configure using the override credentials when needed.

Create `ca_device_auth_nso` Credential Profile

Create a new credential profile in Cisco NSO for the special access user that you created in section [Creating a special access user in NSO](#) of this guide. Add the HTTP and HTTPS credentials for the user in this credential profile. The snapshot below the user and password specification for user, “`cwuser`”.

The screenshot shows the configuration interface for a credential profile named `ca_device_auth_nso`. The profile name is entered in a text field. Below it, there is a section titled "Add Credential Protocols" containing two rows of configuration fields:

Connectivity Type	User Name *	Password *	Confirm Password *
HTTPS	cwuser	*****	*****
HTTP	cwuser	*****	*****

Each row includes a dropdown for connectivity type, a text field for the username, and two password fields (one for the password and one for confirmation), all with eye icons for visibility toggles. A trash icon is present to the right of each row. At the bottom left, there is a "+ Add Another" link. At the bottom right, there are "Save" and "Cancel" buttons.

IMPORTANT

Along with the `ca_device_auth_nso` credential profile, you will have another credential profile in DLM which would specify the user/pass information to Cisco NSO for all other components of Cisco Crosswork. In the example below, this credential profile is called “`nso-creds`”.

Important: Ensure that the username for regular DLM credential profile is different from the username in the `ca_device_auth_nso` profile.

Profile Name * nso-creds

Add Credential Protocols

This username should be different from the username of the ca_device_auth_nso cred profile

Connectivity Type	User Name *	Password *	Confirm Password *
SSH	admin	*****	*****
Enable Password			
TELNET	admin	*****	*****
Enable Password			
NETCONF	admin	*****	*****
HTTP	admin	*****	*****

+ Add Another

Add DLM Provider Property

Once you have created the credential profile in DLM, you need to add a property to all the Cisco NSO providers in DLM which will be used in Crosswork CA. The snapshot below shows the property specification.

Properties for nso



Property Key	Property Value
ca_device_auth_nso	ca_device_auth_nso

Make sure that property key and property value are both set to "ca_device_auth_nso"

Troubleshooting

The following table lists common errors that you could possibly encounter.

No.	Error Substring	Problem	Resolution
1.	nso umap user must also be a nso credential profile user	ca_device_auth_nso username does not match any umap users	<ol style="list-style-type: none"> 1. Add/fix the umap 2. Edit your ca_device_auth_nso cred profile
2.	empty auth group umap from nso	No umap found in the Cisco NSO authgroup	Add the umap
3.	failed to retrieve RESTCONF resource root. please verify NSO <IP> is reachable via RESTCONF	Crosswork CA failed to connect to Cisco NSO via RESTCONF	Ensure that the username/password as specified in ca_device_auth_nso cred profile can connect to Cisco NSO via RESTCONF.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

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: <https://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. (1110R)