Cisco Crosswork Change Automation NSO Function Pack Installation Guide

Version 4.1.0

Contents

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 of this document

This guide describes:

- Installing the **cw-na-fp-ca-4.1.0-nso-5.5.2.9.tar.gz** function pack on Cisco NSO 5.5.2.9 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 4.1.0.

Pre-requisites

The list below shows the minimum versions of the Cisco NSO and Cisco Crosswork with which the Crosswork Change Automation function pack v4.1.0 is compatible.

- Cisco NSO: v5.5.2.9 system install
- Cisco Crosswork: v4.1.0

Install and Configure

The sections below show how to install the **cw-device-auth** function pack on system install Cisco NSO 5.5.2.9 or higher.

Installing Function Pack

1. Download the **cw-device-auth** v4.1.0 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@nso1:~$ ncs_cli -C -u admin
admin connected from 2003:10:11::50 using ssh on nso1
admin@ncs# packages reload
```

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

```
admin@ncs# show packages package cw-device-auth
packages package cw-device-auth
package-version 4.1.0
description     "Crosswork device authorization actions pack"
ncs-min-version [ 5.5.2.9 ]
```

```
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-requites 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/tailf-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.


```
{
  "tailf-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;
             +            }
                      }
                  }
              }
    }
}
cwuser@ncs(config-umap-cwuser)# commit
Commit complete.
```

After the configuration, the authgroup should look like this.

```
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=
 umap cwuser
  callback-node /cw-creds-get
  action-name   get
 !
!
```

Ensure that

- umap is added to an existing authgroup of the device(s) of interest

- The umap is using the correct username.

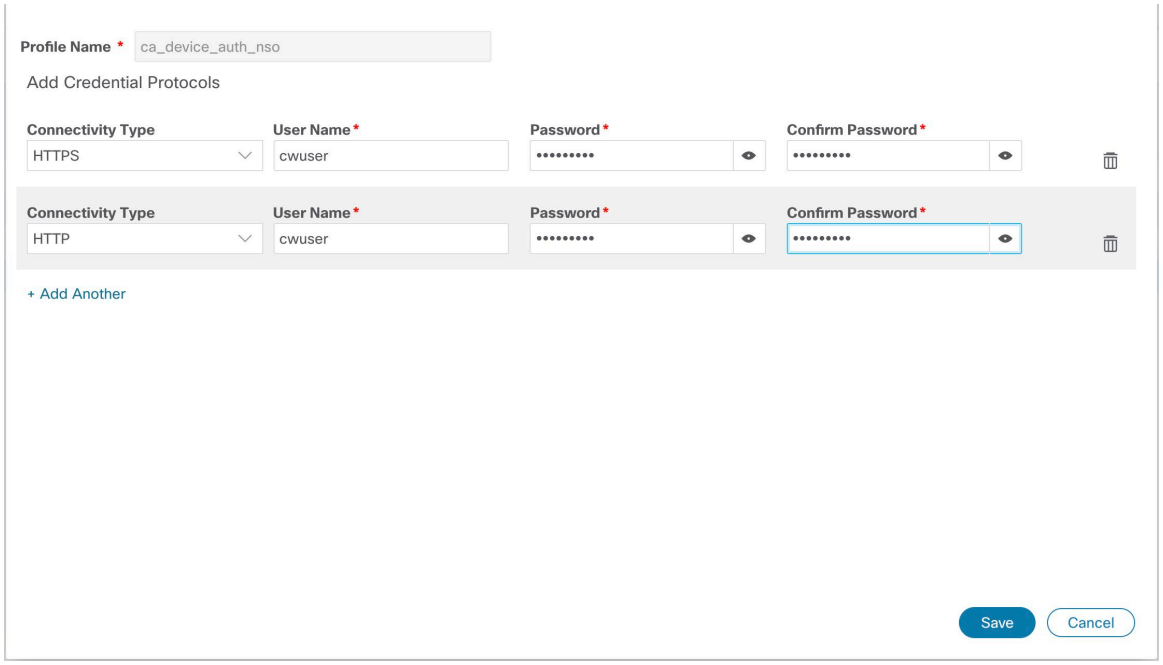
If any of the above is not correct, you will see issues at runtime.

Configuring DLM in CW

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

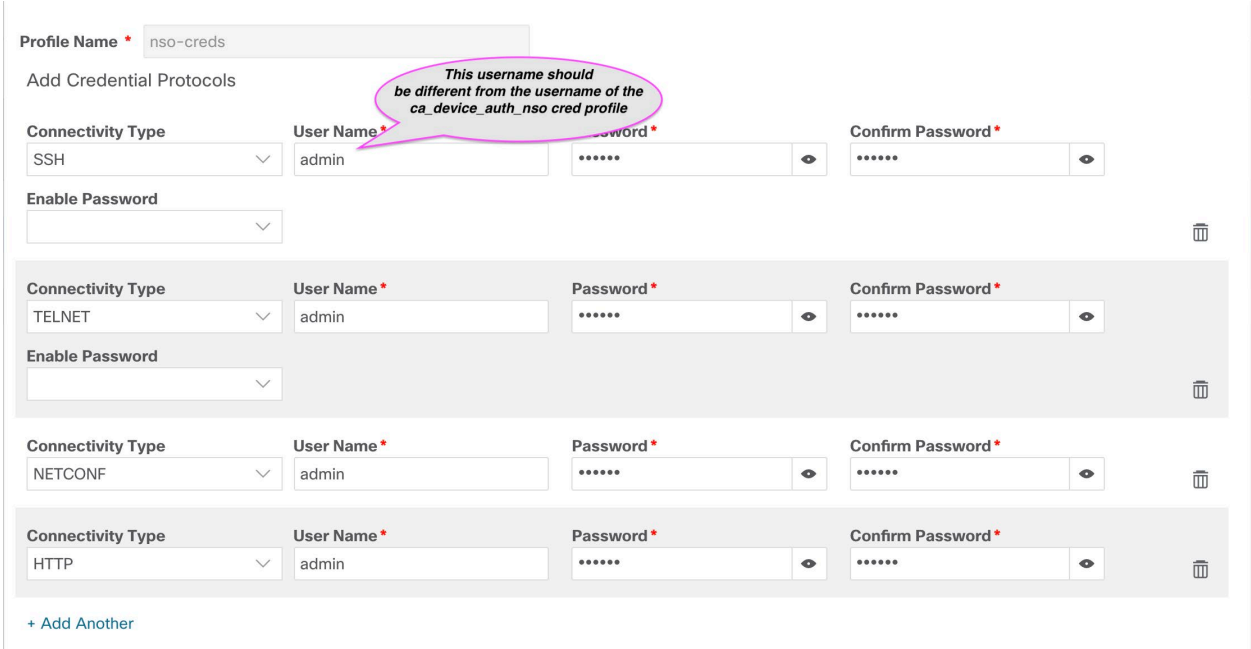
Create a new credential profile in Cisco NSO for the special access user that you created in section **Creating a special access user in NSO** of this guide. Add the HTTP and HTTPS credentials for the user in this credential profile. The snapshot below the user and password specification for user, "cwuser".



P.S. IMPORTANT

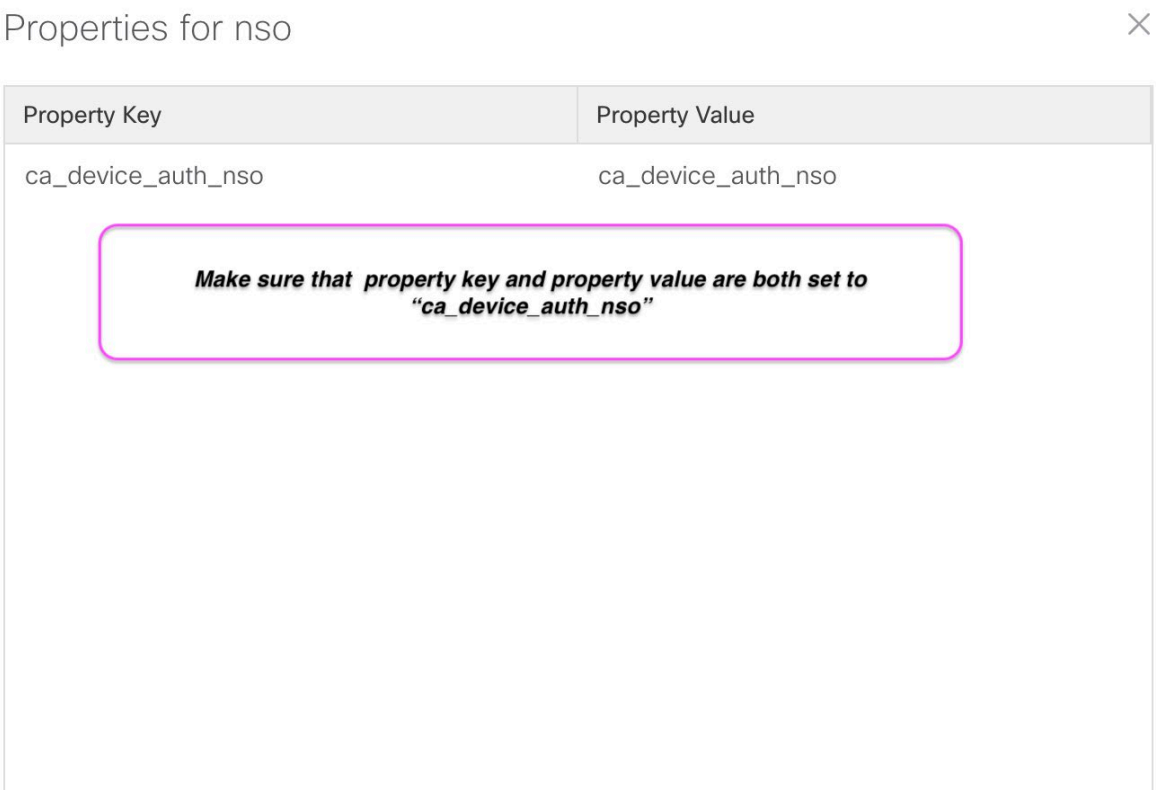
Along with the **ca_device_auth_nso** credential profile, you will have another credential profile in DLM which would specify the user/pass information to Cisco NSO for all other components of Cisco Crosswork. In the example below, this credential profile is called, "**nso-creds**".

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



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.



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	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 **cw_device_auth_nso** cred profile can connect to Cisco NSO via RESTCONF.