Cisco Crosswork Change Automation NSO Function Pack Installation Guide Version 1.0.0

Table of Contents

1 Introduction

This document describes how to download, install, and configure the Change Automation function pack on NSO. Additionally, the document describes the configuration needed from Crosswork for Change Automation.

1.1 Purpose of this document

This guide covers the following topics:

- Installation of cw-device-auth v1.0.0 function pack on NSO 5.4.2 and the associated configurations for the function pack on NSO.
- Section 2.1 covers the authgroup configurations for creating a unique umap for Change Automation.
- Section 3 shows the DLM configurations, and the CA application settings needed in CW 4.0.0

1.2 Pre-requisites

The list below shows the minimum versions of the NSO and Cisco Crosswork with which cw-device-auth v1.0.0 is compatible.

- NSO (Network Service Orchestrator): v5.4.2. System install
- Cisco Crosswork: v 4.0.0

2 Install and Configure

The sections below show how to install the cw-device-auth FP on a system install NSO 5.4.2 or higher.

2.1 Installing Function Pack

1. Download the cw-device-auth v1.0.0 from the repository to your 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 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 1.0.0
 description     "Crosswork device authorization actions pack"
 ncs-min-version [ 5.4.2 ]
 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
```

2.2 Creating a special access user in NSO

Starting Cisco Crosswork 4.0, Cisco Crosswork Change Automation will use a special access user to connect to NSO for all configuration changes. This means that you cannot use the same user as DLM or collection services to access NSO. This section discusses the necessary pre-requites for user creation.

Note: The steps below assume that NSO is running on a ubuntu VM. If your 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 a 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 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]
      }
    }
  ]
}
```


2.3 Adding usermap (umap) to NSO authgroup

NSO allows users to define authgroups for specifying credentials 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 CA override credentials passthrough feature uses this umap. To use CA, a umap configuration needs to be created in the authgroup for the devices.

For example, consider you have a device "**xrv9k-1**" enrolled in 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:

- **umap is added to an existing authgroup of the device(s) of interest**
- **The umap is using the correct username.**

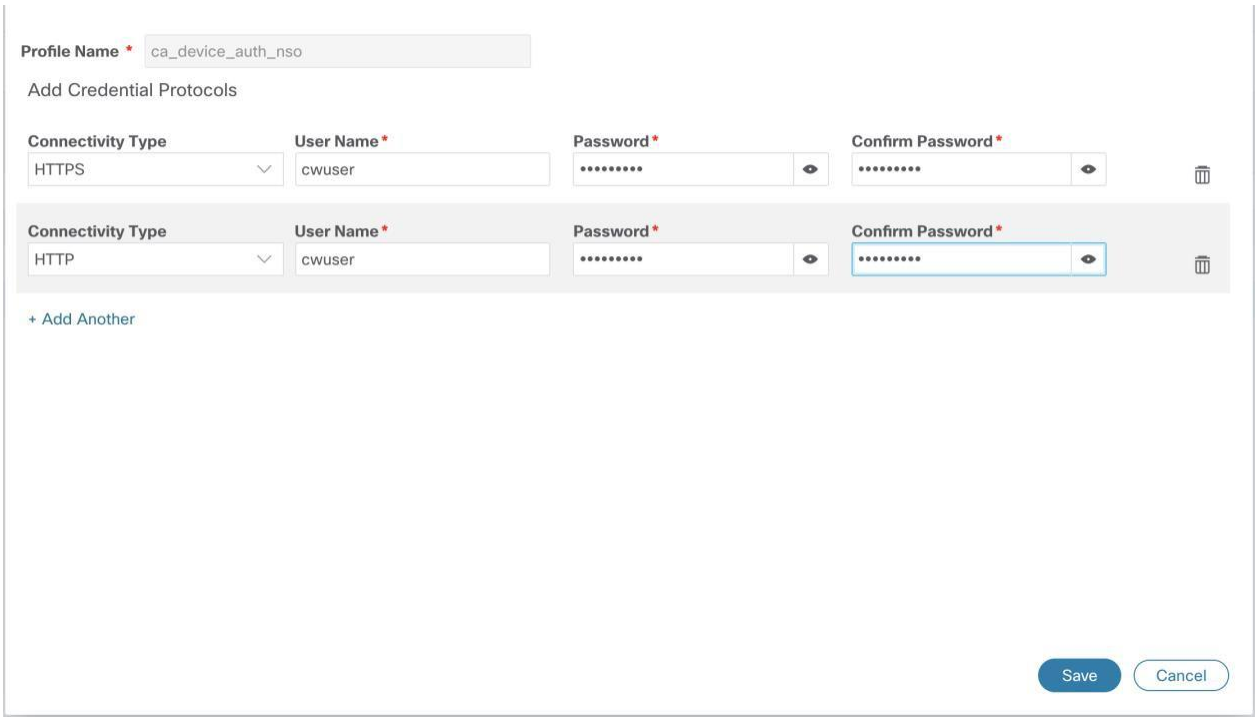
If any of the above is not correct, you will see issue at runtime

3 Configuring DLM in Cisco Crosswork

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

3.1 Create ca_device_auth_nso credential profile

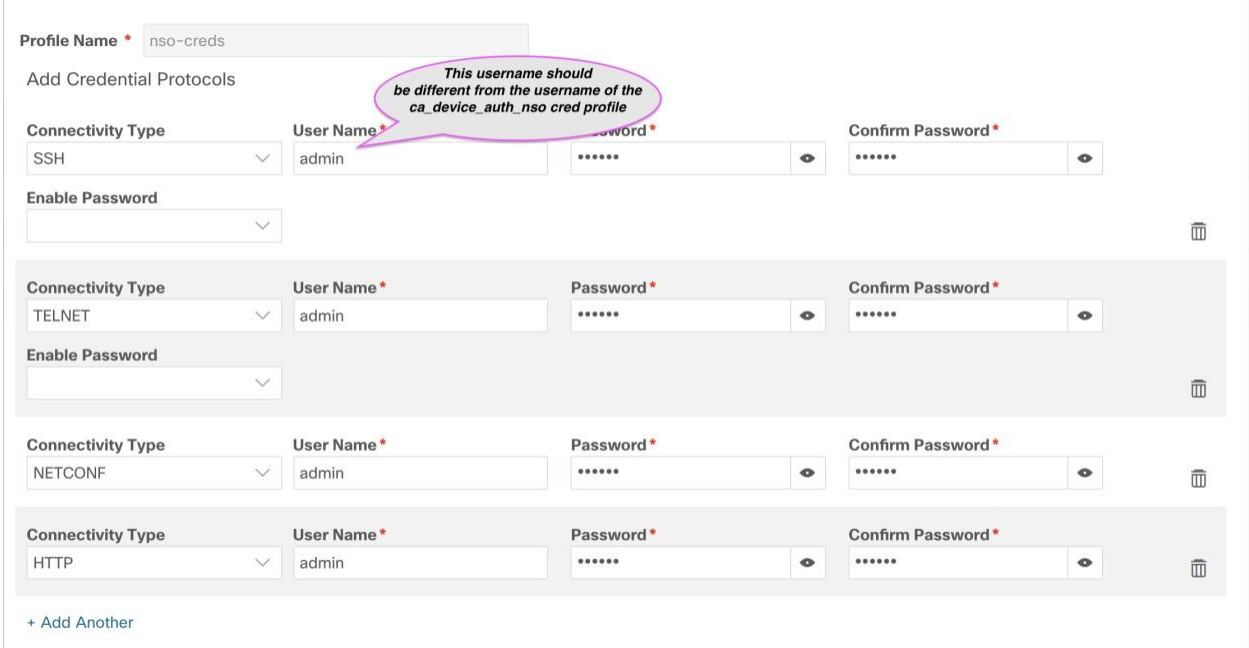
Create a new credential profile in NSO for the special access user that you created in section 2.2 of this guide. Add the HTTP and HTTPS credentials for the user in this credential profile. The snapshot below the user/pass specification for user, "**cwuser**".



IMPORTANT

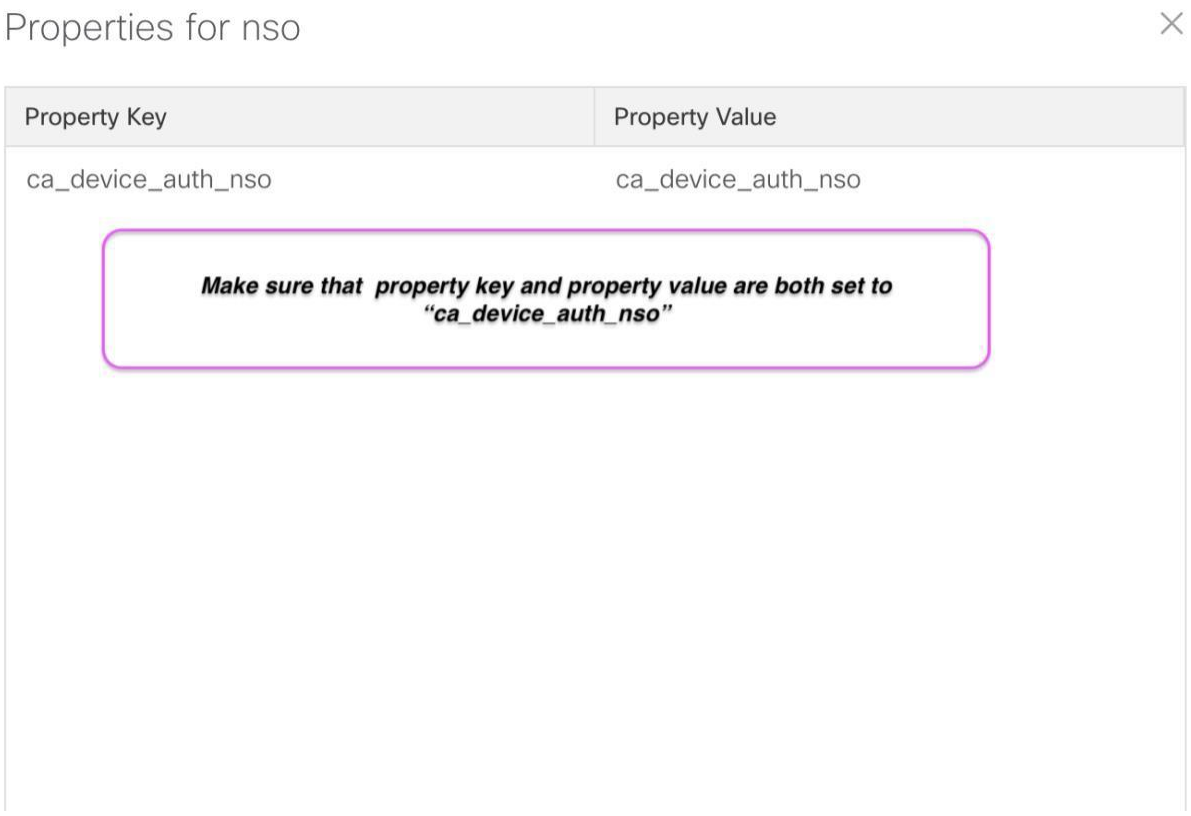
Along with the ca_device_auth_nso credential profile, you will have another credential profile in DLM which would specify the user/pass information to NSO for all other components of Crosswork. In the example below, this credential profile is called, "nso-creds"

MAKE SURE THAT THE USERNAME FOR THE REGULAR DLM CREDENTIAL PROFILE IS DIFFERENT FROM THE USERNAME IN CA_DEVICE_AUTH_NSO PROFILE



3.2 Add DLM provider property

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



4 Troubleshooting

The table below shows some common errors you could 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 NSO authgroup	Add the umap
3.	`failed to retrieve RESTCONF resource root. please verify NSO <IP> is reachable via RESTCONF`	CA failed to connect to NSO via RESTCONF	Ensure that the username/password as specified in cw_device_auth_nso cred profile can connect to NSO via RESTCONF.