Cisco Crosswork Change Automation NSO Function Pack

Installation Guide

Version 6.0.2

Contents

© 2024 Cisco and/or its affiliates. All rights reserved.

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 **ncs-6.1.9-cw-device-auth-6.0.0.tar.gz** function pack on Cisco NSO 6.1.9 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 6.0.2

Pre-requisites

The list below shows the minimum versions of the Cisco NSO and Cisco Crosswork with which the Crosswork Change Automation function pack v6.0 is compatible:

- Cisco NSO: v6.1.9 system install.
- Cisco Crosswork: v6.0.2

© 2024 Cisco and/or its affiliates. All rights reserved.

Installing and Configuring

The sections below show how to install the **cw-device-auth** function pack on system install Cisco NSO 6.1.9 or higher.

Installing Function Pack

1. Download the **cw-device-auth** v6.0.2 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 the reload is complete.

```
admin@ncs# show packages package cw-device-auth
packages package cw-device-auth
package-version 6.0.0
description     "Crosswork device authorization actions pack"
ncs-min-version [ 6.1]
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 an 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' ...
```

© 2024 Cisco and/or its affiliates. All rights reserved.

```
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. Add cwuser to the nacm group

   Note: The nacm rule should be configured with cwuser even though you do not have admin as a user on server.

```
*nacm groups group ncsadmin user-name cwuser

nacm groups group ncsadmin
 user-name [ admin cwuser private ]

* The default permissions are shown like below.

admin@ncs# show running-config nacm
nacm read-default        deny
nacm write-default       deny
nacm exec-default        deny
nacm cmd-read-default    deny
nacm cmd-exec-default    deny
```

3. Ensure that the new user that you created has HTTP and 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 shown below. Any other response would indicate that one more setting before this did not work.

```
{
  "tailf-ncs:package": [
    {
```

© 2024 Cisco and/or its affiliates. All rights reserved.

```
        "name": "cw-device-auth",
        "package-version": "1.0.0",
        "description": "Crosswork device authorization actions pack",
        "ncs-min-version": ["6.0"],
        "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 can contain a default-map or a usermap (umap). Additionally, a umap can be defined in the authgroup for overriding the default credentials from default-map or other umaps.

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
 umap admin
  remote-name     cisco
  remote-password $9$LzskzrvZd7LeWwVNGZTdUBDdKN7IgVV/UkJebwM1eKg=
 !
```

© 2024 Cisco and/or its affiliates. All rights reserved.

```
    !
```

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

```
    cwuser@ncs# config
    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
     umap admin
      remote-name     cisco
      remote-password $9$LzskzrvZd7LeWwVNGZTdUBDdKN7IgVV/UkJebwM1eKg=
     !
     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.
- umap is using the correct username.

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

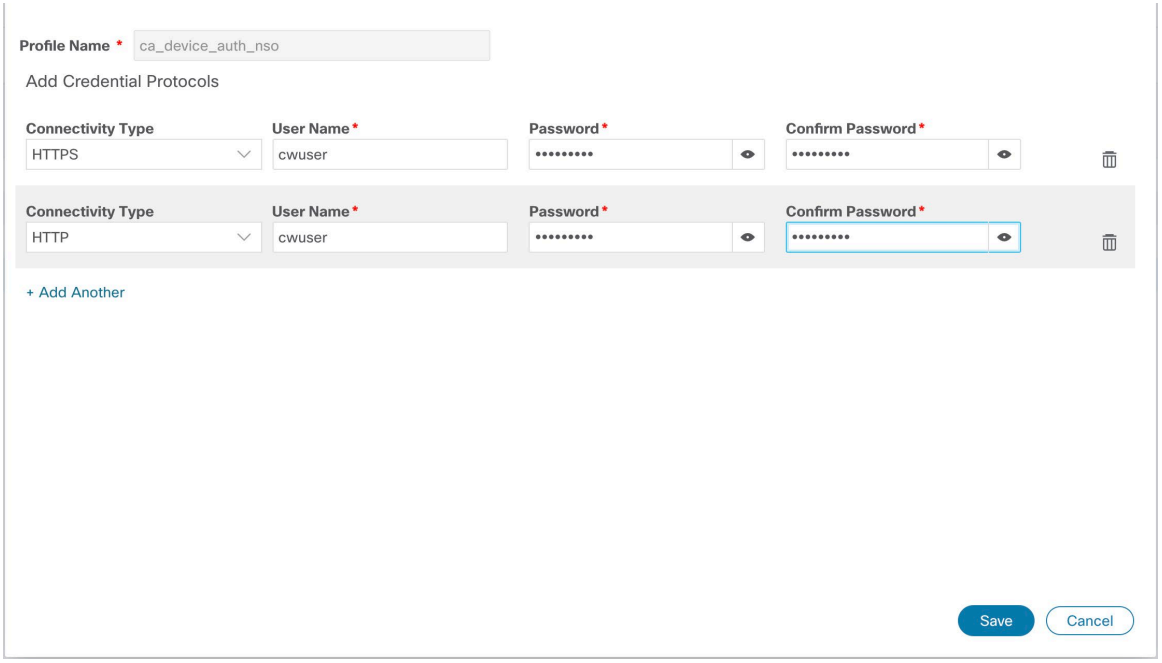
© 2024 Cisco and/or its affiliates. All rights reserved.

Configuring DLM in Cisco Crosswork

After installing and configuring the function pack in Cisco NSO, you need to set up 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 image below shows the user and password specification for user, "**cwuser**".

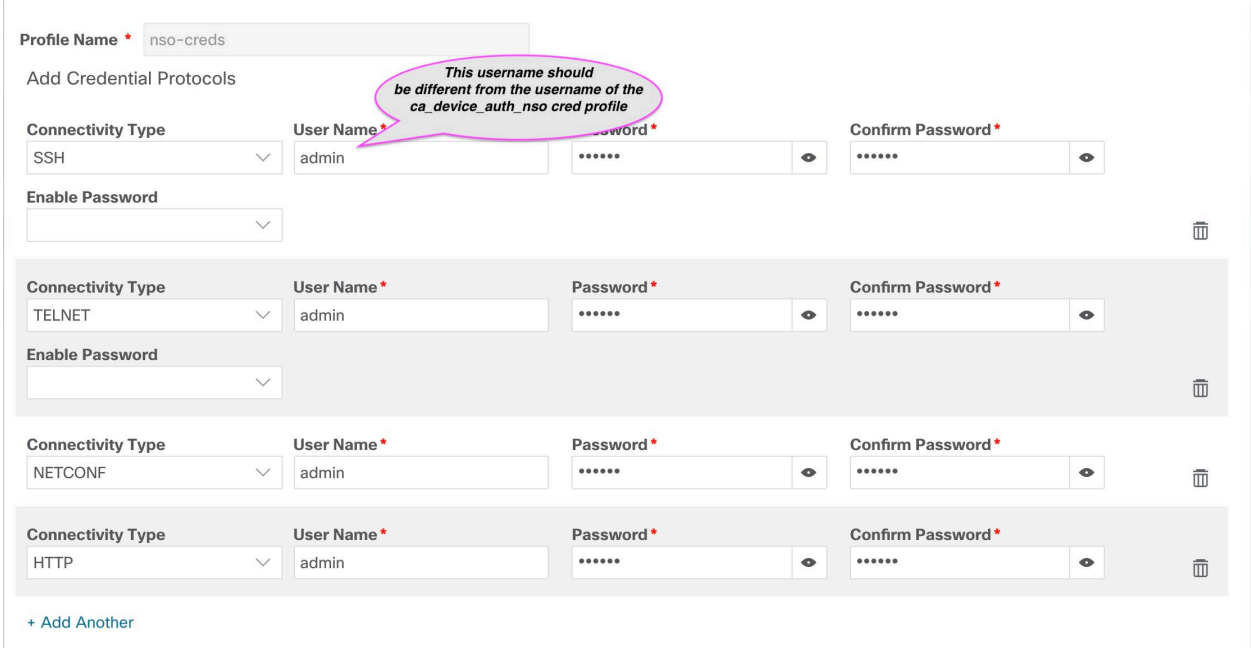


IMPORTANT

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

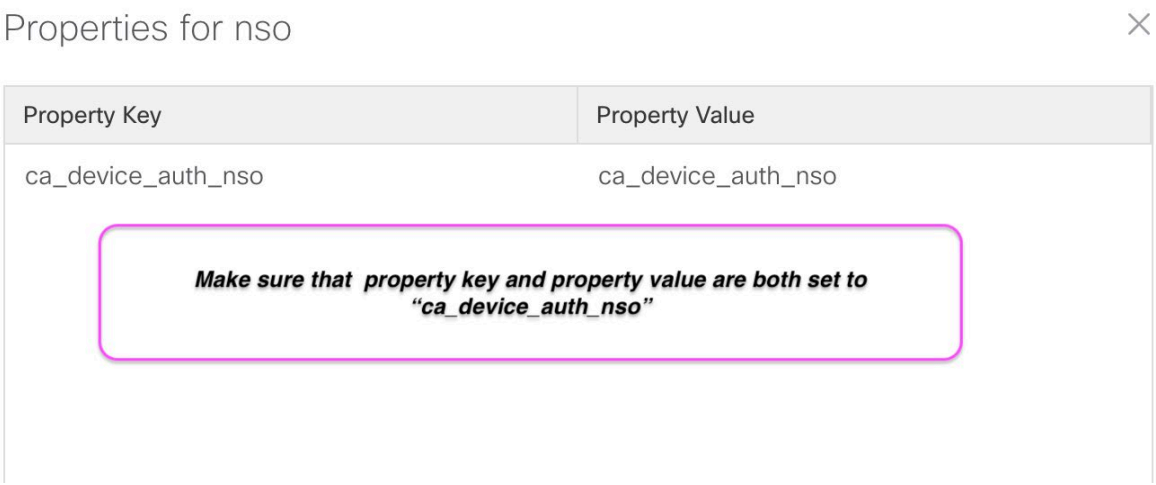
Important: Ensure that the username for regular DLM credential profile is different from the username in the **ca_device_auth_nso** profile.

© 2024 Cisco and/or its affiliates. All rights reserved.



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 image below shows the property specification.



© 2024 Cisco and/or its affiliates. All rights reserved.

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2024 Cisco and/or its affiliates. All rights reserved.