Providing Credentials
(With Explanatory Screenshots for Each Device Type)

Overview

After adding the devices to the NCM inventory, you need to provide device credentials to establish communication between the device and NCM. Details such as the mode (protocol) through which communication is to be established, port details, login name, password etc. are to be provided. The credentials have to be supplied based on the device type. This step is crucial to get started with NCM. This tutorial provides guidelines on entering the credentials.

How to provide credentials?

To provide credentials for a single device:

1. Go to "Inventory" and select the device for which communication has to be established
2. click 'Credentials' menu on the top bar

In the Credentials UI, provide the details as explained in the following steps.

Step 1: Choose the Protocol

Based on the type of device, you can select any of the following combinations of protocols to establish communication between NCM and the device:

1. **TELNET-TFTP** (Establishing communication with the device via Telnet and transferring the configuration via TFTP)
2. **TELNET** (Establishing communication with the device via TELNET and executing show commands on the device to get configuration details)
3. **SSH-TFTP** (Establishing communication with the device via SSH and transferring the configuration via TFTP)
4. **SSH-SCP** (Establishing communication with the device via SSH and transferring the configuration via SCP)
5. **SSH** (Establishing communication with the device via SSH and executing show commands on the device to get configuration details)
6. **SNMP-TFTP** (Establishing communication with the device via SNMP and transferring the configuration via TFTP)
Step 2: Provide other credentials based on protocol choice

Credentials for TELNET-TFTP, TELNET, SSH-TFTP, SSH-SCP & SSH

The following screenshots depict how to enter the credentials for the devices. For ease of understanding, the screenshots illustrate how the credentials are entered while accessing the device via a telnet console and explain how the same values are entered in the NCM GUI.

Important Note: Refer to the screenshots available from page 5 before proceeding with entering the credentials

User Credential Profile

If you have downloaded NCM and carrying out the settings for the first time, you may skip this 'User Credential Profile' step.

NCM offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. The Common Credentials are known as profiles. For more details, click here.

Credentials have been split into two divisions:

Primary Credentials - deal with parameters that are necessary to establish communication with the device. Details such as Login Name, Password, Prompt, Enable UserName, Enable Password and Enable Prompt are classified as basic details.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login Name</td>
<td>While establishing connection with a device, if the device asks for a Login Name, set a value for this parameter. This parameter is Optional.</td>
</tr>
<tr>
<td>2</td>
<td>Password</td>
<td>To set the Password for accessing the device.</td>
</tr>
<tr>
<td>3</td>
<td>Prompt</td>
<td>The prompt that appears after successful login.</td>
</tr>
<tr>
<td>4</td>
<td>Enable UserName</td>
<td>When entering into privileged mode, some devices require UserName to be entered. Provide the username if prompted; otherwise leave this field empty.</td>
</tr>
<tr>
<td>5</td>
<td>Enable Password</td>
<td>This is for entering into privileged mode to perform configuration operations like backup/upload. This parameter is mandatory.</td>
</tr>
<tr>
<td>6</td>
<td>Enable Prompt</td>
<td>This is the prompt that will appear after going into enable mode.</td>
</tr>
</tbody>
</table>

Additional Credentials - certain parameters usually take standard values. All such parameters have been classified under 'Additional Credentials'. Port, login prompt, enable
userprompt, password prompt, enable password prompt values are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details. Providing TFTP Server Public IP / SCP Server Public IP if the device is behind NAT/firewall has also been classified under Additional Credentials.

Click the link "Additional Credentials" to view/enter values for these parameters. Except TFTP/SCP Server Public IP, all other parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TFTP / SCP Server Public IP</td>
<td>When the device is present outside the private network (i.e. when the private IP of NCM is not reachable for the device) this parameter can be used to provide the public IP of the NCM server (NAT’ed IP of NCM). This IP will be used in Configuration backup via TFTP / SCP.</td>
</tr>
<tr>
<td>2</td>
<td>Telnet/SSH Port</td>
<td>Port number of Telnet/SSH - 23 (for Telnet) and 22 (for SSH) by default.</td>
</tr>
<tr>
<td>3</td>
<td>Login Prompt</td>
<td>The text/symbol that appears on the console to get the typed login name is referred as login prompt. For example, Login:</td>
</tr>
<tr>
<td>4</td>
<td>Password Prompt</td>
<td>The text displayed on the console when asking for password. For example, Password:</td>
</tr>
<tr>
<td>5</td>
<td>Enable User Prompt</td>
<td>The text displayed on the console when asking for Enable UserName. For example, UserName:</td>
</tr>
<tr>
<td>6</td>
<td>Enable Password Prompt</td>
<td>The text displayed on the console when asking for password. For example, Password:</td>
</tr>
</tbody>
</table>

- After providing the credentials, if you want to take a backup of the device immediately after updating the credentials, select the 'backup' checkbox
- Click 'Save & Test' if you want to test the validity of the credentials; otherwise, click "Update" to apply the values
- The chosen credentials would be applied to the Device

Once you complete this step - that is, providing credentials, you will find the credentials icon 🗒 beside the device name in the inventory.
Credentials for SNMP-TFTP

User Credential Profile

If you have downloaded NCM and carrying out the settings for the first time, you may skip this 'User Credential Profile' step.

NCM offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. The Common Credentials are known as profiles. For more details, click here.

Primary Credentials for SNMP-TFTP

<table>
<thead>
<tr>
<th>S.No</th>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SNMP Port</td>
<td>Port number of SNMP - 161 by default.</td>
</tr>
</tbody>
</table>
| 2    | Read Community        | An SNMP community is a group of managed devices and network management systems within the same administrative domain. Each SNMP request packet includes a community name. When a request packet is received, the remote access server looks for the name in its community table:  
  - If the name is not found, the request is denied and an error is returned.  
  - If the name is found, the associated access level is checked and the request is accepted if the access level is high enough for the request.  
  
  The SNMP Read Community string is like a user id or password that allows Read-only access to the device. |
| 3    | Write Community       | The SNMP Write Community string is like a user id or password that allows Read and Write access to the devices. |

Additional Credentials

Click the link "Additional Credentials" to view/enter values for these parameters. Except TFTP/SCP Server Public IP, all other parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TFTP / SCP Server</td>
<td>When the device is present outside the LAN (i.e. when the private IP of NCM is not reachable for the device) this parameter</td>
</tr>
<tr>
<td>Public IP</td>
<td>can be used to provide the public IP of the NCM server (NAT’ed IP of NCM). This IP will be used in Configuration backup via TFTP.</td>
<td></td>
</tr>
</tbody>
</table>

**Explanatory Screenshots**

**Example 1: Cisco IOS Device - Password and Enable Password configured**

![Explanatory Screenshot 1]

**Example 2: Cisco IOS Device – Directly going to Enable Mode**

![Explanatory Screenshot 2]
Example 3: Cisco CatOS Device - Password and Enable Password configured

Example 4: Cisco CatOS Device – Directly going to Enable Mode
Example 5: Cisco VPN Concentrator

Example 6: 3Com Router
Example 7: Nortel BayStack

Example 8: NetScreen Firewall
Example 9: Juniper Router

Example 10: HP Procurve Switch
Example 11: Foudry Switch

Example 12: Fortinet Fortigate Firewall
Step 3: Testing the Validity of Credentials

Credential values entered through the Credentials GUI should be accurate. Otherwise, NCM will not be able to establish connection with the device. To ensure the correctness of credential values, NCM provides the testing option. After entering the credentials, you can test the values during which NCM will indicate if the values entered are valid. It will pinpoint the invalid values and you can carry out corrections accordingly.

To test the validity of credentials,

- After providing the credentials, click 'Update & Test'
- This updates the credential values in the DB and then carries out the testing. The result of the testing will be shown in a separate window as below:

![Test Credentials - Windows Internet Explorer](image)

- The testing result indicates valid credential values with a green 'tick' mark. The invalid values are marked as red cross marks. You need to change the invalid values. Alongside, the CLI command execution result (through which NCM ascertains the validity of credential values) is also displayed.
- If you want to test the validity of credentials of a device which has already been given credentials, select the particular device in the inventory, click 'Credentials'. In the Device Credentials page that opens up, click "Test Credentials". Rest is same as above.

**Note:** The credential testing option is provided only for TELNET-TFTP, TELNET, SSH and SSH-TFTP protocols.
Sharing Common Credentials Across Devices

In practical applications, you may find that the same set of credentials could well be applied 'as they are' to many devices. In such cases, to avoid the cumbersome task of entering the credentials for each device separately, NCM offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. This is called as 'Credential Profile'.

Credential Profile can be created as a ready-to-use format called simply as 'Profiles'. You can create a profile with a specific name. Once you create a credential profile, its name will automatically be listed in the drop-down menu in the "Credentials" UI for the field "Use Profile". When you wish to use the profile, if you just choose the corresponding profile in the drop-down menu, all the credential information will be automatically filled-up.

Creating Credential Profiles

To create Credential Profiles,

1. Go to "Admin" >> "Device Management" >> "Credential Profile" >> "New Profile" (Alternatively, you can click the "Add New" action item present beside the 'Use profile' drop-down in the Inventory ---> Credentials GUI).
2. In the 'Add Credential Profile' GUI that opens,
   - Provide a Name for the new credential profile that has to be created. This is the name that will appear in the "Use Profile" drop-down
   - Provide a description for the profile. Though this is for reference purpose, filling up this field is mandatory to avoid confusion at any future point of time
   - Fill-up credential values for the desired protocol. [Refer to the description provided above for information about the parameters and guidelines on choosing the values] and click the "Add". The New Credential Profile is created

Managing Credential Profiles

Go to "Admin" >> "Device Management" >> "Credential Profile" to edit/remove a profile or to view the devices referred by a profile.