

## 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.

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


**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.

S.No	Credential	Description
1	TFTP / SCP Server Public IP	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.
2	Telnet/SSH Port	Port number of Telnet/SSH - <b>23</b> (for Telnet) and <b>22</b> (for SSH) by default.
3	Login Prompt	The text/symbol that appears on the console to get the typed login name is referred as login prompt. For example, Login:
4	Password Prompt	The text displayed on the console when asking for password. For example, Password:
5	Enable User Prompt	The text displayed on the console when asking for Enable UserName. For example, UserName:
6	Enable Password Prompt	The text displayed on the console when asking for password. For example, Password:

- 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

S.No	Credential	Description
1	SNMP Port	Port number of SNMP - 161 by default.
2	Read Community	<p>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:</p> <ul style="list-style-type: none"> <li>• If the name is not found, the request is denied and an error is returned.</li> <li>• 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.</li> </ul> <p>The SNMP Read Community string is like a user id or password that allows Read-only access to the device.</p>
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.

S.No	Credential	Description
1	TFTP / SCP Server	When the device is present outside the LAN (i.e. when the private IP of NCM is not reachable for the device) this parameter

	Public IP	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.
--	-----------	---

## Explanatory Screenshots

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

The screenshot shows a Telnet session for a Cisco2611 device. The user enters 'enable' and then a password. The 'Apply Credentials' dialog box is open, showing the configuration for a TELNET profile. The 'Options' section has 'Primary' selected. The 'Use Credential Profile' is set to '---Select---'. The 'Login Name' field is empty. The 'Password' field contains '\*\*\*\*\*'. The 'Enable UserName' field is empty. The 'Enable Password' field contains '\*\*\*\*\*'. The 'Enable Prompt' field contains '#'. A checkbox for 'Backup the device immediately after updating the credentials' is checked.

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

The screenshot shows a Telnet session for a Cisco2811 device. The user enters 'admin' as the username and a password. The 'Apply Credentials' dialog box is open, showing the configuration for a TELNET profile. The 'Options' section has 'Primary' selected. The 'Use Credential Profile' is set to '---Select---'. The 'Login Name' field contains 'admin'. The 'Password' field contains '\*\*\*\*\*'. The 'Enable Prompt' field contains '#'. The 'Enable UserName' and 'Enable Password' fields are empty. A checkbox for 'Backup the device immediately after updating the credentials' is unchecked.

### Example 3: Cisco CatOS Device - Password and Enable Password configured

The screenshot displays the 'Apply Credentials' dialog box for a Telnet connection to a Cisco CatOS device. The dialog is configured with the following settings:

- Protocol:** TELNET
- Options:** Primary (selected), Additional
- Use Credential Profile:** ---Select---
- Login Name:** (empty)
- Password:** \*\*\*\*
- Prompt (?):** >
- Enable UserName:** (empty)
- Enable Password:** \*\*\*\*
- Enable Prompt (?):** enable
- Backup the device immediately after updating the credentials:** (unchecked)

The background shows a Telnet session with the following commands and responses:

```
Telnet cisco-catos
Welcome to our company
Password: *****
cisco-catos > enable
Password: *****
cisco-catos < enable >
```

Orange arrows indicate the mapping between the terminal output and the configuration fields in the dialog box.

### Example 4: Cisco CatOS Device – Directly going to Enable Mode

The screenshot displays the 'Apply Credentials' dialog box for a Telnet connection to a Cisco CatOS device. The dialog is configured with the following settings:

- Protocol:** TELNET
- Options:** Primary (selected), Additional
- Use Credential Profile:** ---Select---
- Login Name:** admin
- Password:** \*\*\*\*
- Prompt (?):** enable
- Enable UserName:** (empty)
- Enable Password:** (empty)
- Enable Prompt (?):** (empty)
- Backup the device immediately after updating the credentials:** (unchecked)

The background shows a Telnet session with the following commands and responses:

```
Telnet cisco5509
Welcome to our company
Username: admin
Password: *****
cisco5509 < enable >
```

Orange arrows indicate the mapping between the terminal output and the configuration fields in the dialog box.

## Example 5: Cisco VPN Concentrator

**Apply Credentials**

Protocol: TELNET

Options:  Primary  Additional

Use Credential Profile: ---Select---

Login Name: admin

Password: \*\*\*\*\*

Prompt (?): enable

Enable UserName:

Enable Password:

Enable Prompt (?):

Backup the device immediately after updating the credentials

New Profile

## Example 6: 3Com Router

**Apply Credentials**

Protocol: TELNET

Options:  Primary  Additional

Use Credential Profile: ---Select---

Login Name: manager

Password: \*\*\*\*\*

Prompt (?): :

Enable UserName:

Enable Password:

Enable Prompt (?):

Backup the device immediately after updating the credentials

New Profile

### Example 7: Nortel BayStack

The screenshot shows a Telnet session with the title "Telnet foundry2402". The terminal output displays the Nortel BayStack boot sequence, including the prompt "Enter Ctrl-Y to begin." and system information such as "BayStack 380-24T", "Nortel Networks", "Copyright (c) 1996-2003, All Rights Reserved", and hardware details "HW:01 FW:3.0.0.2 SW:v3.0.1.04".

Overlaid on the right is the "Apply Credentials" configuration window. The "Protocol" is set to "TELNET". Under "Options", the "Primary" radio button is selected. The "Use Credential Profile" dropdown is set to "---Select---". The "Login Name" field is empty, "Password" is masked with "\*\*\*\*\*", and "Prompt" is set to "option". There are checkboxes for "Enable UserName", "Enable Password", and "Enable Prompt", all of which are currently unchecked. A checkbox at the bottom is labeled "Backup the device immediately after updating the credentials". A green "New Profile" button is located in the top right corner of the window.

### Example 8: NetScreen Firewall

The screenshot shows a Telnet session with the title "Telnet netscreen-208". The terminal output shows the login prompt "Username: admin" and "Password: \*\*\*\*\*", followed by the "netscreen-208 >" prompt. Orange arrows point from the terminal input to the corresponding fields in the "Apply Credentials" window.

The "Apply Credentials" window is identical to the one in Example 7, but with the following specific configurations: "Login Name" is "admin", "Password" is masked with "\*\*\*\*\*", and "Prompt" is ">". The "Backup the device immediately after updating the credentials" checkbox is unchecked. The "New Profile" button is visible in the top right.



### Example 9: Juniper Router

The screenshot shows a Telnet session with a Juniper Procurve switch. The terminal output is as follows:

```
Telnet procurve2524  
HEWLETT - PACKARD COMPANY 3000  
Username : manager  
Password : *****  
procurve2524 #
```

Orange arrows point from the terminal text to the corresponding fields in the 'Apply Credentials' dialog:

- Username: manager
- Password: \*\*\*\*\*
- Prompt: #

The 'Apply Credentials' dialog is configured with the following settings:

- Protocol: TELNET
- Options: Primary (selected), Additional
- Use Credential Profile: ---Select---
- Login Name: manager
- Password: \*\*\*\*\*
- Prompt (?): #
- Enable UserName: (empty)
- Enable Password: (empty)
- Enable Prompt (?): (empty)
- Backup the device immediately after updating the credentials: (unchecked)

### Example 10: HP Procurve Switch

The screenshot shows a Telnet session with an HP Procurve switch. The terminal output is as follows:

```
Telnet procurve2524  
HEWLETT - PACKARD COMPANY 3000  
Username : manager  
Password : *****  
procurve2524 #
```

Orange arrows point from the terminal text to the corresponding fields in the 'Apply Credentials' dialog:

- Username: manager
- Password: \*\*\*\*\*
- Prompt: #

The 'Apply Credentials' dialog is configured with the following settings:

- Protocol: TELNET
- Options: Primary (selected), Additional
- Use Credential Profile: ---Select---
- Login Name: manager
- Password: \*\*\*\*\*
- Prompt (?): #
- Enable UserName: (empty)
- Enable Password: (empty)
- Enable Prompt (?): (empty)
- Backup the device immediately after updating the credentials: (unchecked)

## Example 11: Foundry Switch

The screenshot shows a Telnet session to a Foundry switch (foundry2402) and the corresponding 'Apply Credentials' dialog in ManageEngine Password Manager Pro.

**Telnet Session:**

```
Telnet foundry2402
"Foundry FastIron Edge 2
User Access Verification

Please Enter Password : *****
User login successful.
foundry2402 > enable
Password : *****
foundry2402 #
```

**Apply Credentials Dialog:**

- Protocol: TELNET
- Options: Primary (selected), Additional
- Use Credential Profile: ---Select---
- Login Name: (empty)
- Password: \*\*\*\*\*
- Prompt: >
- Enable UserName: (empty)
- Enable Password: \*\*\*\*\*
- Enable Prompt: #
- Backup the device immediately after updating the credentials:

Red arrows indicate the mapping between the Telnet session and the dialog fields: Password (\*\*\*\*\*), Prompt (>), Enable Password (\*\*\*\*\*), and Enable Prompt (#).

## Example 12: Fortinet Fortigate Firewall

The screenshot shows a Telnet session to a Fortinet Fortigate Firewall (foundry2402) and the corresponding 'Apply Credentials' dialog in ManageEngine Password Manager Pro.

**Telnet Session:**

```
Telnet foundry2402
Welcome to our company
Login : admin
Password : *****
foundry2402 #
```

**Apply Credentials Dialog:**

- Protocol: TELNET
- Options: Primary (selected), Additional
- Use Credential Profile: ---Select---
- Login Name: admin
- Password: \*\*\*\*\*
- Prompt: #
- Enable UserName: (empty)
- Enable Password: (empty)
- Enable Prompt: (empty)
- Backup the device immediately after updating the credentials:

Red arrows indicate the mapping between the Telnet session and the dialog fields: Login Name (admin), Password (\*\*\*\*\*), and Prompt (#).

### 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 carryout 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:

Credential	Given Value	Validity
Port	23	✓
Login Prompt	:	✓
Login Name		✓
Password Prompt	:	✓
Password	*****	✓
Prompt	>	✓
Enable Username Prompt		✓
Enable Username		✓
Enable Password Prompt	:	✓
Enable Password	*****	✓
Enable Prompt	#	✓

```

enable
Password: *****
Cisco805# copy startup-config tftp
Address or name of remote host []? 192.168.117.244
Destination filename [startup-config]? 5_ConfigFile.txt
!!
2395 bytes copied in 0.76 secs
Cisco805#
  
```

**Test Credential Status**  
 ✓ Credentials are valid.

- 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 **"Settings" >> "Device Management" >> "Add Credential"** (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 **"Settings" >> "Device Management" >> "Credential Profile"** to edit/remove a profile or to view the devices referred by a profile.



**ZOHO Corp.** (formerly AdventNet Inc.)

4900 Hopyard Rd., Suite 310, Pleasanton, CA 94588, USA **Phone:** +1-925-924-9500 **Fax:** +1-925-924-9600

**Website:** <http://www.networkconfigurationmanager.com>

**For Queries:** [ncm-support@manageengine.com](mailto:ncm-support@manageengine.com)