



Getting Started Guide

Getting Started with n-Command

Welcome to the n-Command software.

n-Command is an intuitive, scalable software suite that delivers productivity tools that aid in managing NetVanta-based networks. n-Command is designed to help IT administrators ease the burden of daily network operations and configuration management. This system delivers time saving features that offer the ability to push mass configuration changes and firmware upgrades; backup and restore device configurations; and manage device inventory and Access Control Lists to ADTRAN AOS (ADTRAN Operating System) devices.

n-Command also supports configuration backup/restore and firmware upgrade for ADTRAN Total Access 600 series and Total Access 850 products.

n-Command delivers all of these features and more in a low cost, intuitive, and scalable solution.

This document provides general workflow information to help you get started with the n-Command software. For complete product documentation, see your n-Command online help (select **Help > n-Command Help**).

Step 1: Setting Up Folders

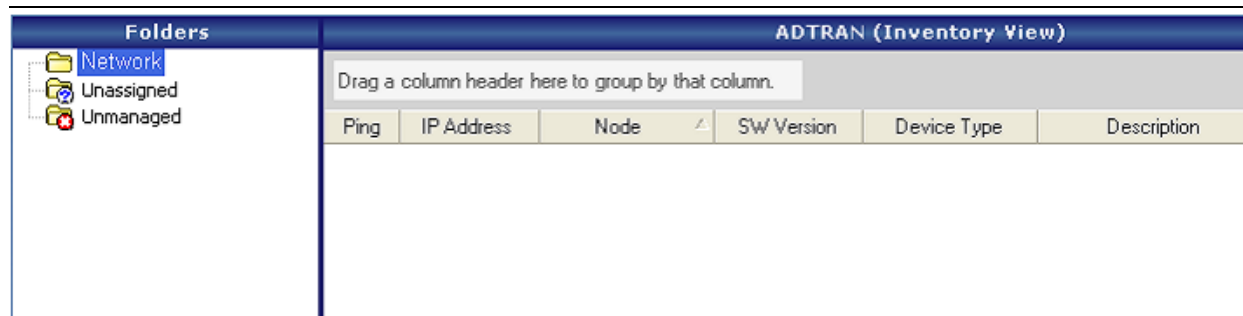
When you start n-Command for the first time, three folders display:

- **Network:** The **Network** folder is the default folder that displays after initial installation. You can change the folder name, delete the folder, or add subfolders.
- **Unassigned:** During device discovery, if you did not select a target folder, AOS/Total Access devices will be placed in the **Unassigned** folder. Once devices are in this folder, you can drag them to different folders for better network organization. You cannot modify or delete the name of this folder.
- **Unmanaged:** All non-AOS/Total Access devices are placed in the **Unmanaged** folder during the discovery process. This folder gives you a view of the other devices found on the network during device discovery. Devices in this folder are not managed by n-Command, but you can drag devices into a managed folder. You cannot modify or delete the name of this folder.



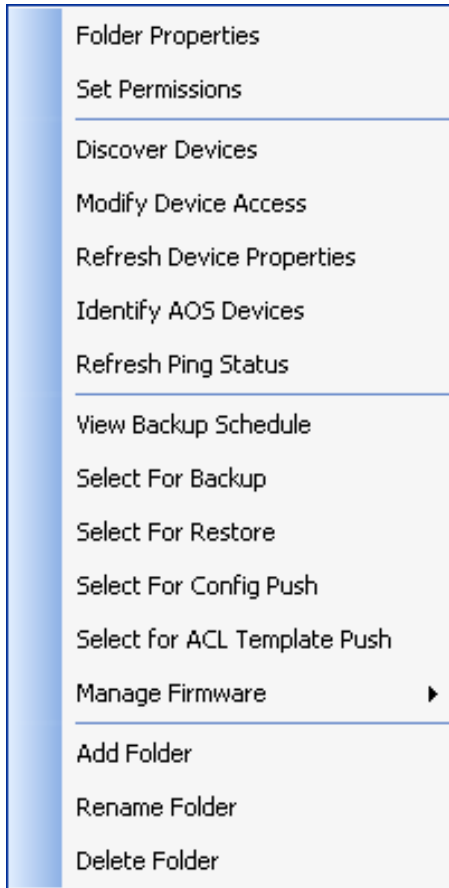
*AOS devices with Simple Network Management Protocol (SNMP) disabled will also be placed in the **Unmanaged** folder. Use the **Identify AOS** command to identify the AOS devices with SNMP disabled. Once identified, use the **Push Configuration** feature to enable SNMP on those devices.*

When you first start n-Command, all of the folders will be empty.

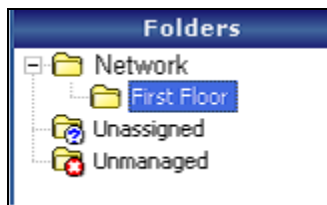


Begin by thinking about how you want to structure your folders. You can create separate folders for different areas of your building, for different types of devices, or any other grouping you want to use.

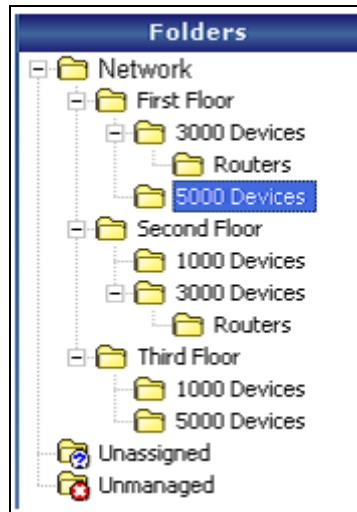
1. When you are ready to start creating your folder structure, right-click the **Network** folder (you can rename the **Network** folder if necessary). The following menu displays:



2. Select **Add Folder**.
3. A new folder displays under the **Network** folder. Type in the name for the new folder (**First Floor** in this example).



- You can add as many folders as necessary, using any structure and naming scheme that is appropriate for your network.



Step 2: Setting Up Users



Only a **Root** user can add other **Root** and **Admin** users. Only a **Root** or **Admin** user can add a new basic **User**.

- Select the **Administration** tab.
- Select **Add New User**.
- Fill in the required information about the new user. The **Username**, **System Role**, and **Default Permissions** fields are required. However, the other fields will help you keep track of the users.



If you plan to add the user to the address book for event notification, enter their e-mail address in the appropriate field.

- Change the user role if necessary. The roles are defined below:
 - Root:** The default user available when n-Command is first started has permission to create other root users, administrators, and basic users. The root user has all administrative privileges. It is a good idea to have at least two root users for security purposes.
 - Admin:** The Administrator can create new users, set up the folder structure, discover devices, and organize devices into folders. **Admin** users generally perform system administration tasks.
 - User:** The **User** can perform basic operations on devices (if they have permission). This includes backing up devices, restoring devices, pushing configuration changes, and performing other non-administrative tasks.

5. If the new user is set to **User**, you will need to set the default permissions (**Root** and **Admin** automatically have all privileges). The options are **View** (view only) and **Unit Manage** (allows users to perform management tasks).
6. A “disable” option is available if a user is out of the office or does not need access to the system for a period of time. To disable a user, select the **Disabled** check box.
7. When you are finished, select **Save User**.
8. When a prompt displays asking if you want to confirm saving the new user, select **Yes**. The user is created, and the new user information displays at the top of the screen. The user’s folder permissions also display.



When a new user first logs in, the user will not have a password. The user will be prompted to set a password the first time he or she logs in.

Step 3: Setting Permissions

Users will have their default permissions (**Unit Manage** or **View**) in all folders. However, you can customize permissions for all folders except for **Unmanaged**.

1. Select the **Network** tab.
2. Select the folder for which you want to set permissions.
3. Select **Set Permissions**. In the bottom of the window, the **Folder Properties** action pane displays.
4. You can change the source for the user’s permissions for each individual folder by selecting an option from **Permission Source**. **Inherit from Parent** uses the permissions set in parent folders or the **Administration** section of the interface. **Custom for this Folder** allows you to set different permissions for accessing devices in folders. If you select **Custom for this Folder**, use the drop-down menu under the **Role** column to change the user’s permissions.
5. The **Role** menu allows you to specify that the user can **Manage Units** or **View** the contents of the folder.



*You can only change this option if **Permission Source** is set to **Custom for this folder**.*



When you change permissions in a folder, all of the subfolders inherit the new permission settings.

6. Select **Save** when you are finished making changes.



*After you set user permissions for folders, you can quickly review a particular user's permissions for all of the folders. Select the **Administration** tab, and then select the user. All of the user's folder permissions display in the lower part of the screen.*

Step 4: Setting Up Device Access (For AOS Devices Only)

Now you need to define device access so n-Command can communicate with the AOS devices on your network. n-Command uses both CLI commands and SNMP to perform certain functions. In order to access AOS devices, a user account is needed and SNMP must be enabled. n-Command can use an existing user account, or a new user account can be created for the device or on the RADIUS Server.



*Creating a new user account for AOS devices can easily be accomplished using the **Config Push** command. First, use an existing user account to initiate communication with AOS devices, and then add a new n-Command user account using **Config Push**. Once added, n-Command can use the new **Username** and **Password**. For detailed information, refer to your n-Command online help.*

Create a Device Username and Password

The **CLI Access** option defines the Username and Password for logging into devices.

1. Select the **Administration** tab.
2. Select **Manage Access Defaults**.
3. Under the **CLI Access** tab, create a username and password for logging into devices on your network.
4. Select the **SSH** option to use SSH instead of Telnet as the default method to send and receive commands.
5. After entering the username and password, select **Save**.



*Username and password for the Total Access 600 Series and Total Access 850 are included as part of the discovery file and is not set up using **Manage Device Access**.*

Create an Enable Password (For AOS Devices Only)

This option defines Enable passwords you can associate with specific devices.

1. Select the **Enable Passwords** tab.
2. The default label is selected. n-Command uses this default password to access all devices unless you specifically create a new label and associate that label's password to the appropriate device or devices. The labels help you identify the different passwords.
3. Enter the new password you want to use in the **Password** field.
4. Enter the same password again in the **Confirm Password** field.
5. To create a new label for devices that will not use the default password, select the **New** button. The cursor displays in the **Label** field.
6. Enter a new label for the new Enable password.
7. Select **Save**, and the new password label displays in the top portion of the window.



*After device discovery, if all devices do not use the default Enable password, you can select the appropriate Enable password label for devices by using the **Network Tab > Modify Device Access** command.*

Create SNMP Strings (For AOS Devices Only)

The **SNMP Strings** option defines the SNMP strings n-Command uses to access the SNMP variables within devices.

1. Select the **SNMP Strings** tab.
2. For both the **Read Communities** and **Read/Write Communities**, select **Add**, and the **Add** window displays. Enter a name for the new SNMP string.
3. Select **OK**. The new string displays in the main window.
4. Use the arrows to change the priority of the strings. n-Command attempts the SNMP access with the top string first. If the top string fails, n-Command will then move down the list to the next string until it gains access to the device. Once access is made, n-Command will associate the appropriate SNMP string to the device.

Step 5: Discovering Devices

After you have set up your folder structure, you can discover the devices on your network.

Select the folder where you want discovered AOS/Total Access devices to be located. Right-click the folder and select **Discover Devices** (see the n-Command help file for detailed information about this option).



For AOS Device Discovery:

*If SNMP is not activated in the target devices, n-Command will discover the devices using Ping, but will mark them as unknown. These devices can be identified as AOS devices by using the **Identify AOS Devices** command. The **Config Push** feature of n-Command, which includes an **Enable Base SNMP** script, can then be used to enable SNMP on the identified AOS devices.*



*If you did not create a folder structure, you can discover devices by right-selecting the **Network** or **Unassigned** folders and selecting **Discover Devices**. You can later move devices into the appropriate folders.*

Step 6: Modifying Device Access (For AOS Devices Only)

If you use different enable passwords across devices, you will need to associate the proper Enable password label with the correct devices. If you have not already created Enable password labels in n-Command, refer to *Step 4: Setting Up Device Access (For AOS Devices Only)*.

1. Select the **Network Tab**.
2. Select the **Modify Device Access** link under **Basic Tasks** in the navigation bar.
3. Select the devices that require a new Enable password label, and drag them to the **Selected Folders/Devices** window.
4. Use the drop-down menus to select the appropriate **SNMP Strings** or **Enable Password Label** for the selected devices. Refer to page 7 for information on how to add more SNMP strings or Enable password labels to the drop-down menus.
5. Select **Save**, and the devices in the selection window will disappear, signaling that the changes have been saved.

Step 7: Configuring E-mail Settings

E-mail must be set up if you intend to send e-mail notification with task completion summaries.

1. Select the **Administration** tab.
2. Select the **E-mail** tab from the **System Preferences** menu.
3. Enter the DNS name of the SMTP e-mail server.
4. If desired, modify the default **From** address.
5. The connection to the e-mail server can be verified using **Test E-mail Server**.
6. Send a test e-mail using the **Send Test E-mail** function.

You can now start working with your network. Refer to your online documentation (**Help > n-Command Help**) to see the other options available in the n-Command software.

Trademarks

n-Command is a trademark and NetVanta is a registered trademark of ADTRAN, Inc. Any brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.