

# Tripp Lite NetCommander-AXS Tutorial and Overview

---

NetCommander-AXS Version 1.0 svn ver. 121

## Contents

Introduction.....	4
Overview.....	4
Prerequisites.....	4
Quick Start .....	5
Install Software.....	5
Discover Your KVM and/or PDU Devices.....	5
Managing Discovered Results .....	10
Setting Up Groups .....	11
Saving Your Document .....	15
Access Mode and Admin Mode.....	17
Admin Mode.....	17
Access Mode.....	17
Display KVM Targets.....	17
Manipulate PDU Target States .....	19
Reloading Your Document.....	21
NetCommander-AXS Window .....	21
Window Components.....	21
Convenience Features .....	22
Managed Elements.....	22
Document .....	22
Group.....	23
Adding a Group.....	23

Editing a Group .....	24
Deleting a Group .....	25
KVM and PDU Devices .....	25
Adding a KVM Device .....	25
Adding a PDU Device .....	28
Editing a Device .....	32
Deleting Devices .....	32
KVM and PDU Target .....	33
Adding a KVM Target .....	33
Adding a PDU Target .....	34
Editing a Target .....	34
Deleting Targets .....	35
External Hosts .....	35
Defining External Hosts Source .....	35
File-based External Hosts .....	37
File-based External Hosts Configuration Example .....	38
LDAP-based External Hosts .....	39
LDAP-based External Hosts Configuration Example .....	39
DNS-based External Hosts .....	41
DNS-based External Hosts Example .....	42
Using External Hosts .....	42
File-based External Hosts Usage Example .....	43
Device Discovery .....	43
User Authentication .....	48
No Authentication Mode .....	49
Document-Defined User Authentication .....	50
Access Policy .....	52
Selected Devices Example .....	53
Selected Targets Example .....	53
User Groups .....	54
Group with Selected Devices Example .....	55
Group with Selected Targets Example .....	56

Users Groups Tab for Group Examples Above .....	57
Users Tab for Group Examples Above .....	57
Session .....	58
LDAP Authentication .....	58
LDAP Servers.....	59
User Access Policy .....	60
Local Administrator .....	61
Target Authentication .....	62
Session .....	63
Example of LDAP user definition .....	64
RADIUS Authentication .....	64
Onboard Device Configuration.....	65
Multi Device Onboard Configuration Deployment .....	66
Multiple Device Firmware Upgrade .....	68
Reachability .....	68
Admin Mode.....	68
Access Mode.....	69
KVM-to-Power .....	70
KVM Targets Name Synchronization.....	72
Pull Target Names from Device .....	72
Push Target Names to Device.....	73
Additional Functionality .....	73
Find .....	73
Reload.....	74
Preferences.....	74
Ping .....	77
Augmenting Supported PDU Devices .....	78

# Introduction

This document provides:

- A quick start to product use of Tripp Lite's NetCommander-AXS
- Orientation of NetCommander-AXS's main features

## Overview

The NetCommander-AXS provides you with a convenient way to:

- Manage and control your Tripp Lite KVM devices
- Access KVM remote sessions
- Manage outlets of your Tripp Lite PDU devices

The product is easily installed and run from your computer's desktop.

Briefly, NetCommander-AXS is installed within seconds with a simple, standard Microsoft Windows-based install program. After that, NetCommander-AXS launches through a desktop icon or the Windows start menu.

Running NetCommander-AXS in edit mode (known as 'Admin Mode'), allows you to add, edit, and delete Tripp Lite KVM and PDU device definitions identified from your network, either through autodiscovery or manually. The content of this edit session can then be saved as an encrypted data file on a local or network drive.

After that, NetCommander-AXS is typically run in 'Access Mode', providing you, and others, the ability to run KVM sessions as well as view PDU outlet statuses and control the outlets, based on the data file.

Data files can be shared with other users who have NetCommander-AXS installed. Based on your needs, data files can be set up requiring user authentication upon accessing them, or alternatively, with no authentication required.

## Prerequisites

- Computer with Microsoft Windows 7, Windows 8, or Windows 10.
- Java JRE 1.7 +
- Deployed Tripp Lite KVM devices. Models supported:
  - o B072-016-IP2, B072-016-IP4, B072-032-IP2, B072-032-IP4, B072-008-1-IP, B072-016-1-IP, B072-032-IP2-K, B072-032-IP4-K, B070-008-19-IP, B070-016-19-IP, B070-016-19-IP2

- Deployed Tripp Lite PDU devices.

## Quick Start

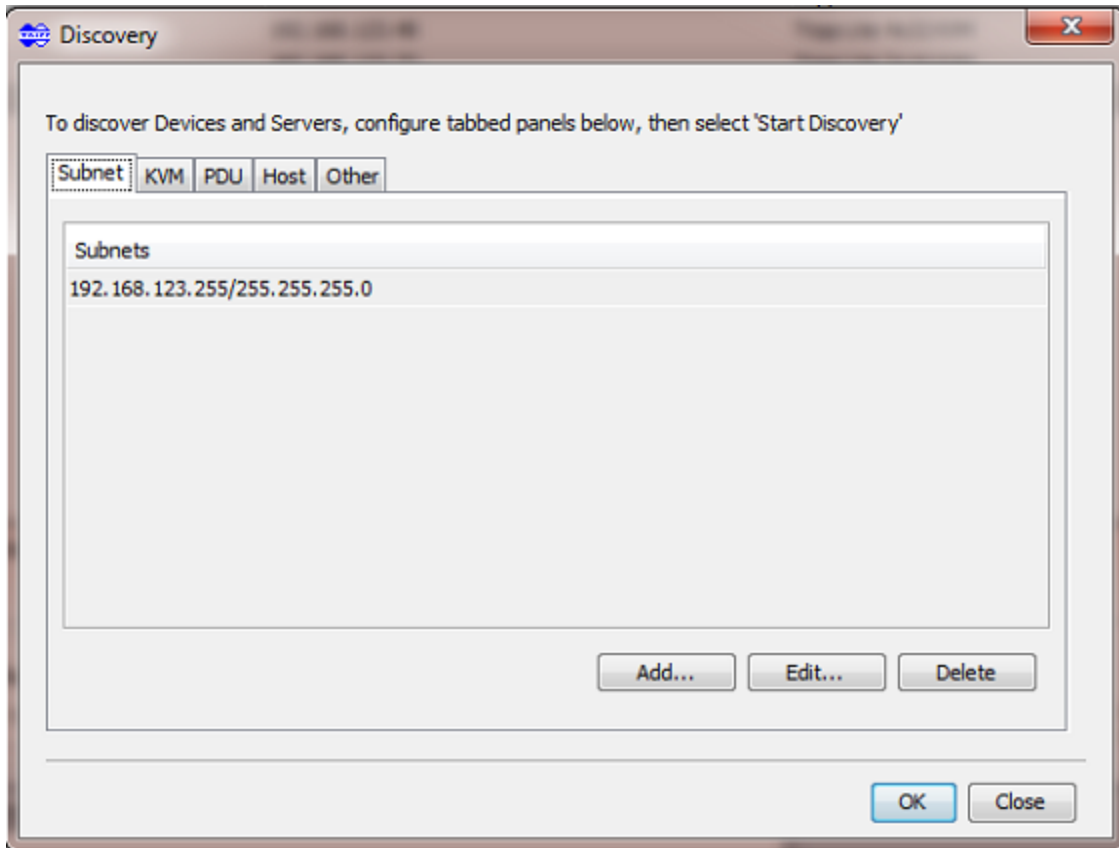
To quickly get up and running, simply follow the steps in the guided example below. Names and IP addresses are provided for simulation only. Your names and IP addresses will be different. For further product explanation, see sections following the Quick Start.

### Install Software

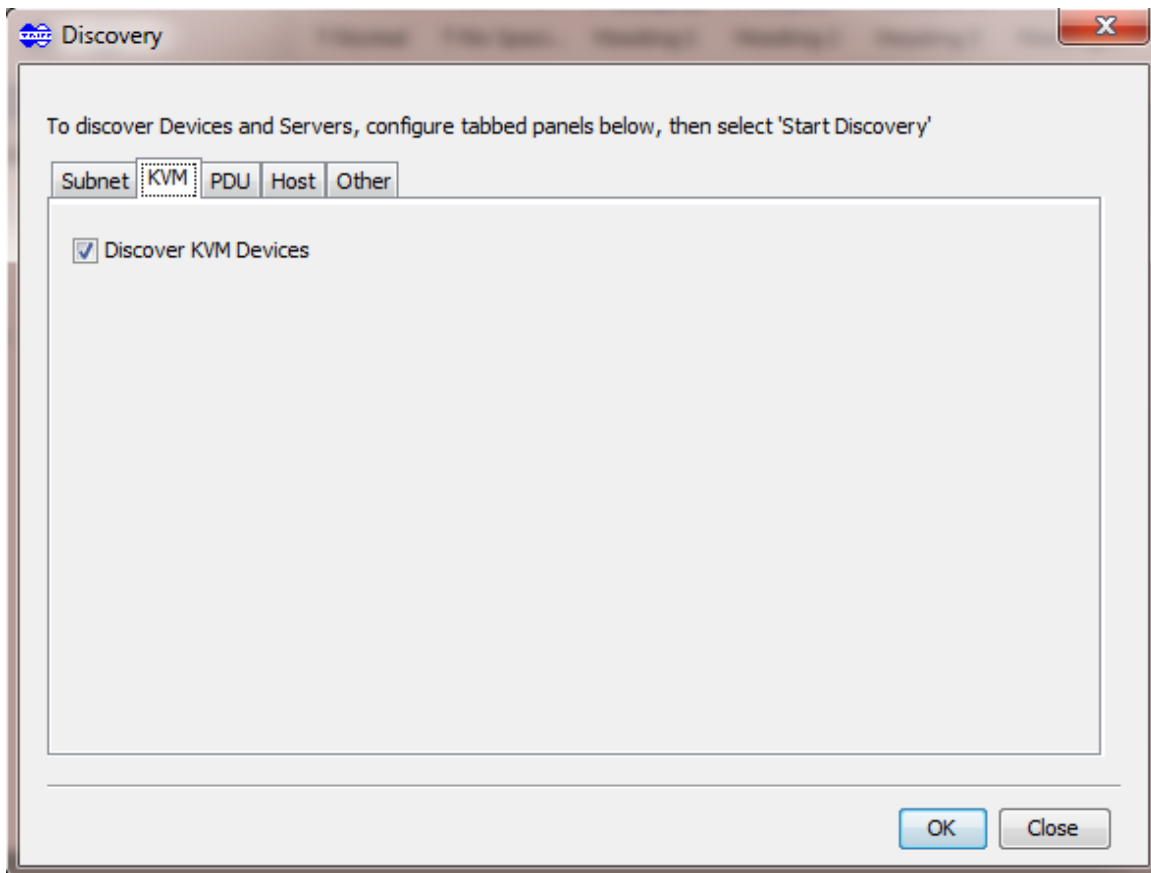
- Install the NetCommander-AXS on your Microsoft Windows PC computer desktop by running the exe installation program
- Start the NetCommander-AXS, and go the next step

### Discover Your KVM and/or PDU Devices

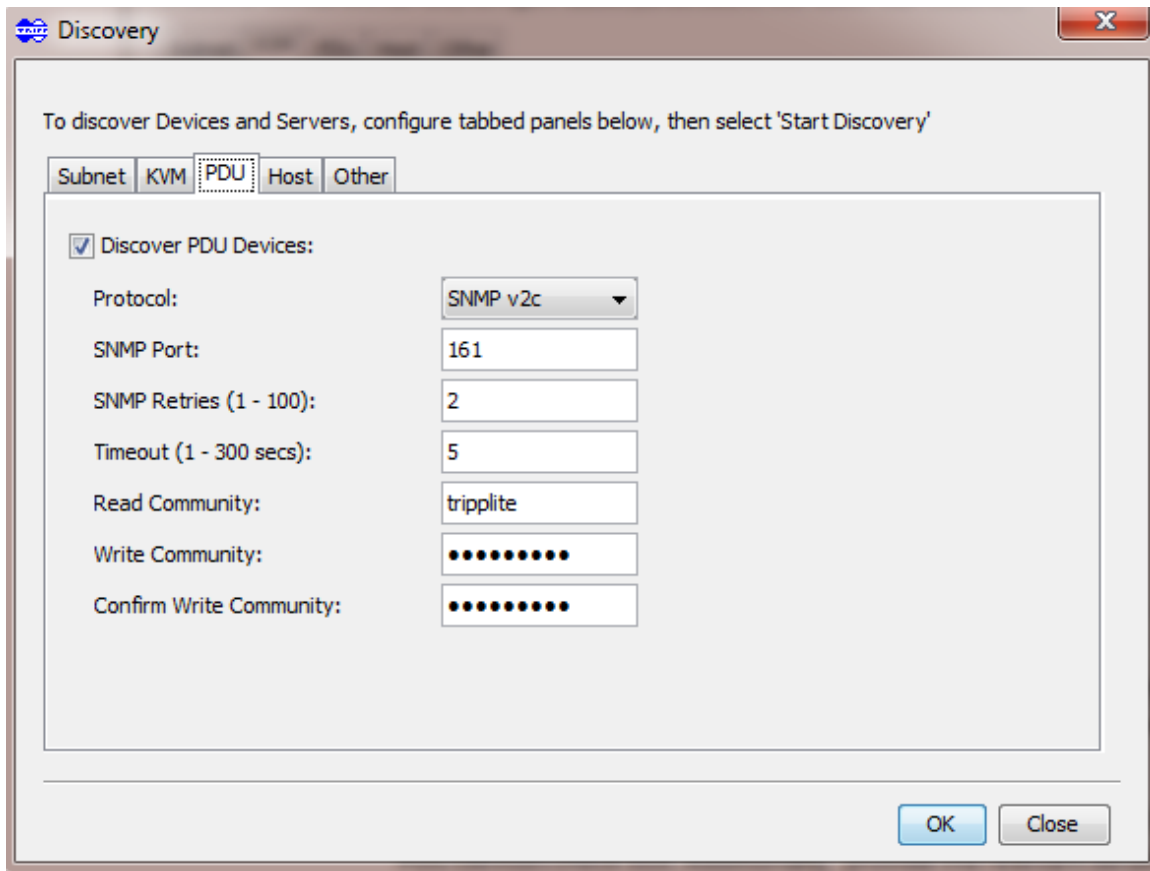
- Starting the NetCommander-AXS for the first time, you will be prompted with a request to discover your Tripp Lite devices. Select 'Yes', and you will be presented with the discovery dialog. Fill out the dialog as follows:
  - In the subnets tab, define the subnet(s) where your Tripp Lite KVM and/or PDU devices are located. Example: If devices are located within subnet 192.168.123.255, then define entry: 192.168.123.255, mask 24 bits. See below:



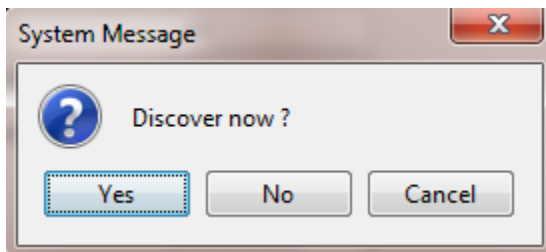
- If you want to discover KVM devices, in the KVM tab, select the 'Discover KVM Devices' check box. See below:



- If you want to discover PDU devices, in the PDU tab, select the 'Discover PDU Devices' check box. Additionally, provide the relevant details for your environment. For the example below, for discovery, it will be assumed that
  - The SNMP protocol is SNMP v2
  - SNMP communications port is 161
  - 2 SNMP retries will be available
  - SNMP communications timeout will be 5 seconds
  - SNMP read community will be triplite
  - SNMP write community will be triplite

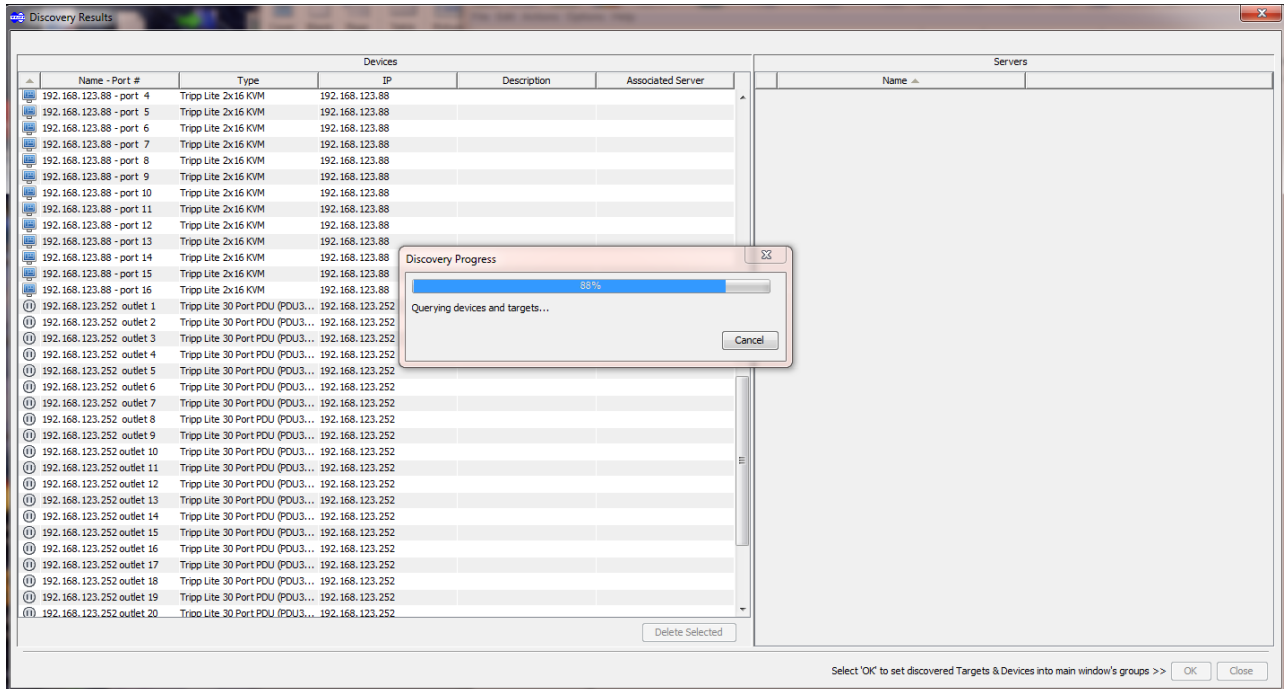


- Next, select the OK button. You will be prompted to confirm the start of discovery. Select 'Yes':



- Now, actual discovery commences. Results of discovery will be populated in a results dialog as they come in. Below is an example of these results:





- Upon completion of discovery, for any discovered KVM devices, device credentials for the devices must be supplied.

You can either:

- Supply the same credentials for all devices, if this is relevant, or
- Supply the credentials for each individual device.

The credentials include device login name, password, and KVM access TCP port

Below is an example of this dialog for the first case:

KVM Device Discovery Completion

To complete discovery of KVM devices below, please provide KVM devices' user name, password, and video TCP port

All discovered KVM devices in table below have the same login name, password, and video TCP port:

User Name:

Password:

Confirm Password:

TCP Port (800-65535):

Discovered KVM Devices:

IP Address ▲	Login Name	Password	TCP Port
192.168.123.73			900
192.168.123.82			900
192.168.123.88			900

OK Cancel

To complete, select 'OK' to close this dialog, and select 'OK' to close the results dialog.

## Managing Discovered Results

The results of the discovery activity are placed in the NetCommander-AXS's main window (the 'Central Manager' window) in its Admin Mode.

This window allows you to view the discovered devices and targets (KVM target endpoints and PDU outlets) by selecting either the 'Devices' or 'Targets' nodes in the left-side tree respectively. Below are examples of discovered devices and targets:

- Discovered Devices:

NetCommander-AXS - New Document \*

File Edit Actions Options Help

TRIPP-LITE

Device Name	IP	Type	Description
192.168.123.73	192.168.123.73	Tripp Lite 2x32 KVM	
192.168.123.82	192.168.123.82	Tripp Lite 1x16 KVM	
192.168.123.88	192.168.123.88	Tripp Lite 2x16 KVM	
192.168.123.252	192.168.123.252	Tripp Lite 30 Port PDU (POU3VSR2)	

Severity	Time	Event	Details
Info	05/07/2016 15:25:39	device added	Device 192.168.123.73 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.82 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.88 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.252 added

- Discovered Targets:

NetCommander-AXS - New Document \*

File Edit Actions Options Help

TRIPP-LITE

Target Name	Device	Port	Description
192.168.123.252 outlet 22	192.168.123.252	22	
192.168.123.252 outlet 23	192.168.123.252	23	
192.168.123.252 outlet 24	192.168.123.252	24	
192.168.123.252 outlet 25	192.168.123.252	25	
192.168.123.252 outlet 26	192.168.123.252	26	
192.168.123.252 outlet 27	192.168.123.252	27	
192.168.123.252 outlet 28	192.168.123.252	28	
192.168.123.252 outlet 29	192.168.123.252	29	
192.168.123.252 outlet 30	192.168.123.252	30	
Aerospace	192.168.123.88	7	
Audmars Piguet Royal Oak	192.168.123.88	15	
Chronomet	192.168.123.88	9	
Constellation	192.168.123.88	6	
DeVille	192.168.123.88	3	
IWC Schaffhausen	192.168.123.88	13	
Navitimer	192.168.123.88	10	
PC 01	192.168.123.82	1	
PC 07	192.168.123.82	7	
PC 11	192.168.123.82	11	
PC 16	192.168.123.82	16	
PloProof	192.168.123.88	5	
Rolex Submariner	192.168.123.88	14	
SeaMaster	192.168.123.88	2	
SeaMaster Planet Ocean	192.168.123.88	4	

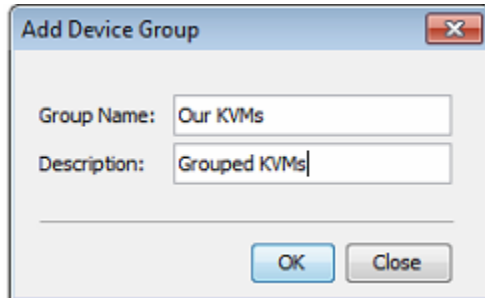
Severity	Time	Event	Details
Info	05/07/2016 15:25:39	device added	Device 192.168.123.73 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.82 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.88 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.252 added

## Setting Up Groups

The discovered results, both the devices and targets, can be organized into logical groupings. Grouping is an optional activity.

## Device Groups

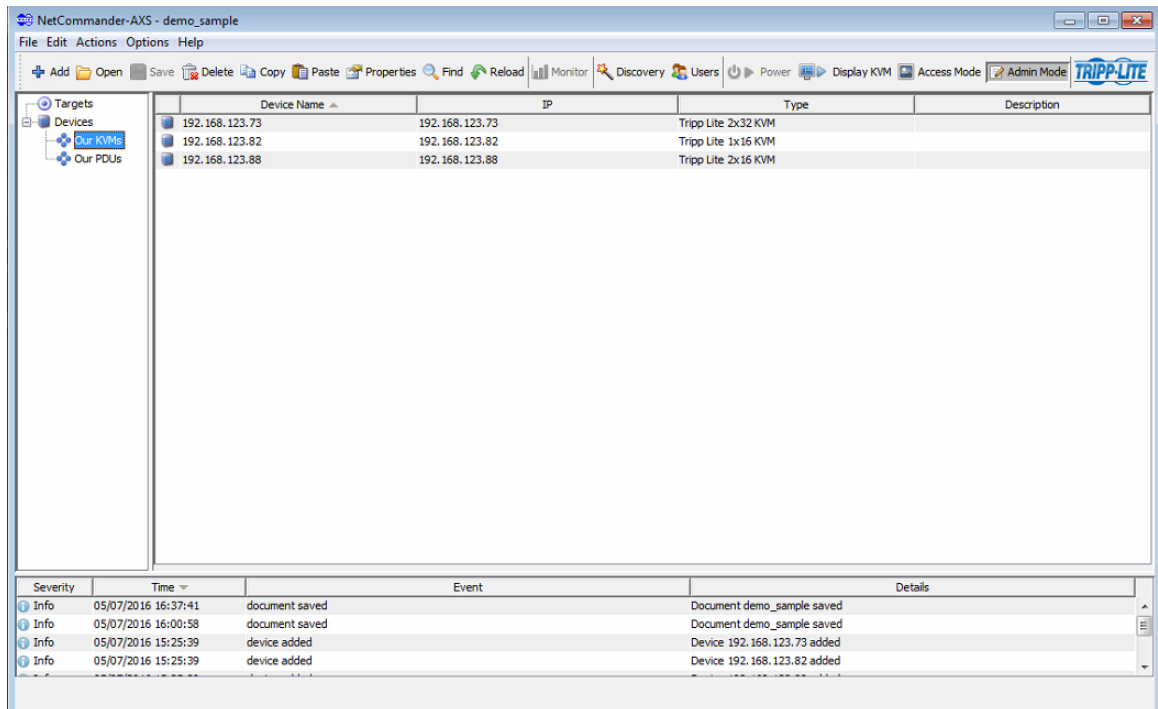
As an example, let's say we want to organize the devices into a group of KVMs and another into a group of PDUs. To do this, select the 'Devices' node in the tree, right-click mouse and select 'Add Group'. Fill out the dialog in a manner similar to as follows, and select 'OK'.



The screenshot shows a dialog box titled "Add Device Group". It has two text input fields: "Group Name" with the value "Our KVMs" and "Description" with the value "Grouped KVMs". At the bottom of the dialog are two buttons: "OK" and "Close".

Drag-and-drop the results into the resulting group. Repeat this activity for another group to be called 'Our PDUs', dragging the PDU devices into it.

Results should be similar to what is shown below for both groups:

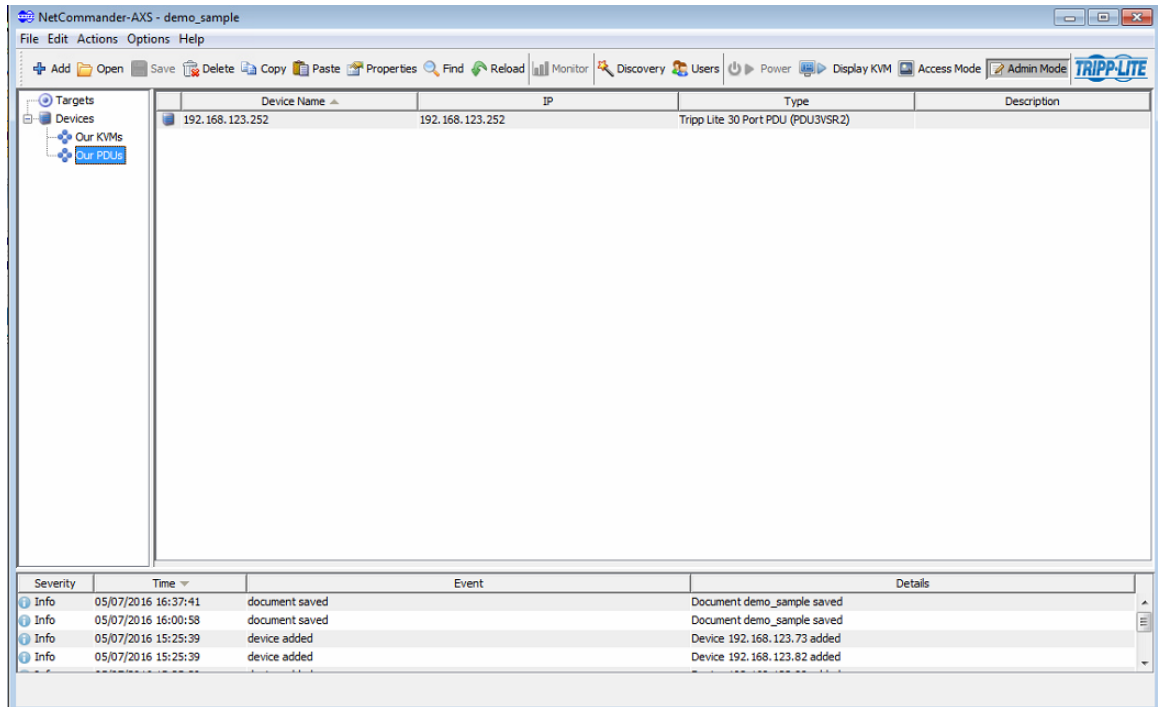


The screenshot shows the NetCommander-AXS interface. The left sidebar shows a tree view with 'Targets' expanded to 'Devices', which contains two sub-groups: 'Our KVMs' and 'Our PDUs'. The main area displays a table of devices:

Device Name	IP	Type	Description
192.168.123.73	192.168.123.73	Tripp Lite 2x32 KVM	
192.168.123.82	192.168.123.82	Tripp Lite 1x16 KVM	
192.168.123.88	192.168.123.88	Tripp Lite 2x16 KVM	

At the bottom of the interface is an event log table:

Severity	Time	Event	Details
Info	05/07/2016 16:37:41	document saved	Document demo_sample saved
Info	05/07/2016 16:00:58	document saved	Document demo_sample saved
Info	05/07/2016 15:25:39	device added	Device 192.168.123.73 added
Info	05/07/2016 15:25:39	device added	Device 192.168.123.82 added



### *Target Groups*

In similar fashion, set up meaningful Target Groups. Let's say, for purposes of example, we want 3 Target Groups: "Power", "Corporate Access", and "Maintenance Access". Let's say all the PDU targets are dragged-and-dropped into "Power", all the KVM targets from the 192.168.123.88 device are dragged-and-dropped into "Corporate Access", and all remaining KVM targets are dragged-and-dropped into "Maintenance Access". Below are sample captures of what these may look like:

NetCommander-AXS - demo\_sample

File Edit Actions Options Help

Add Open Save Delete Copy Paste Properties Find Reload Monitor Discovery Users Power Display KVM Access Mode Admin Mode TRIPP-LITE

Target Name	Device	Port	Description
192.168.123.252 outlet 1	192.168.123.252	1	
192.168.123.252 outlet 2	192.168.123.252	2	
192.168.123.252 outlet 3	192.168.123.252	3	
192.168.123.252 outlet 4	192.168.123.252	4	
192.168.123.252 outlet 5	192.168.123.252	5	
192.168.123.252 outlet 6	192.168.123.252	6	
192.168.123.252 outlet 7	192.168.123.252	7	
192.168.123.252 outlet 8	192.168.123.252	8	
192.168.123.252 outlet 9	192.168.123.252	9	
192.168.123.252 outlet 10	192.168.123.252	10	
192.168.123.252 outlet 11	192.168.123.252	11	
192.168.123.252 outlet 12	192.168.123.252	12	
192.168.123.252 outlet 13	192.168.123.252	13	
192.168.123.252 outlet 14	192.168.123.252	14	
192.168.123.252 outlet 15	192.168.123.252	15	
192.168.123.252 outlet 16	192.168.123.252	16	
192.168.123.252 outlet 17	192.168.123.252	17	
192.168.123.252 outlet 18	192.168.123.252	18	
192.168.123.252 outlet 19	192.168.123.252	19	
192.168.123.252 outlet 20	192.168.123.252	20	
192.168.123.252 outlet 21	192.168.123.252	21	
192.168.123.252 outlet 22	192.168.123.252	22	
192.168.123.252 outlet 23	192.168.123.252	23	
192.168.123.252 outlet 24	192.168.123.252	24	
192.168.123.252 outlet 25	192.168.123.252	25	
192.168.123.252 outlet 26	192.168.123.252	26	
192.168.123.252 outlet 27	192.168.123.252	27	
192.168.123.252 outlet 28	192.168.123.252	28	
192.168.123.252 outlet 29	192.168.123.252	29	
192.168.123.252 outlet 30	192.168.123.252	30	

Severity	Time	Event	Details
Info	05/07/2016 16:45:27	document saved	Document demo_sample saved
Info	05/07/2016 16:37:41	document saved	Document demo_sample saved
Info	05/07/2016 16:00:58	document saved	Document demo_sample saved
Info	05/07/2016 15:25:39	device added	Device 192.168.123.73 added

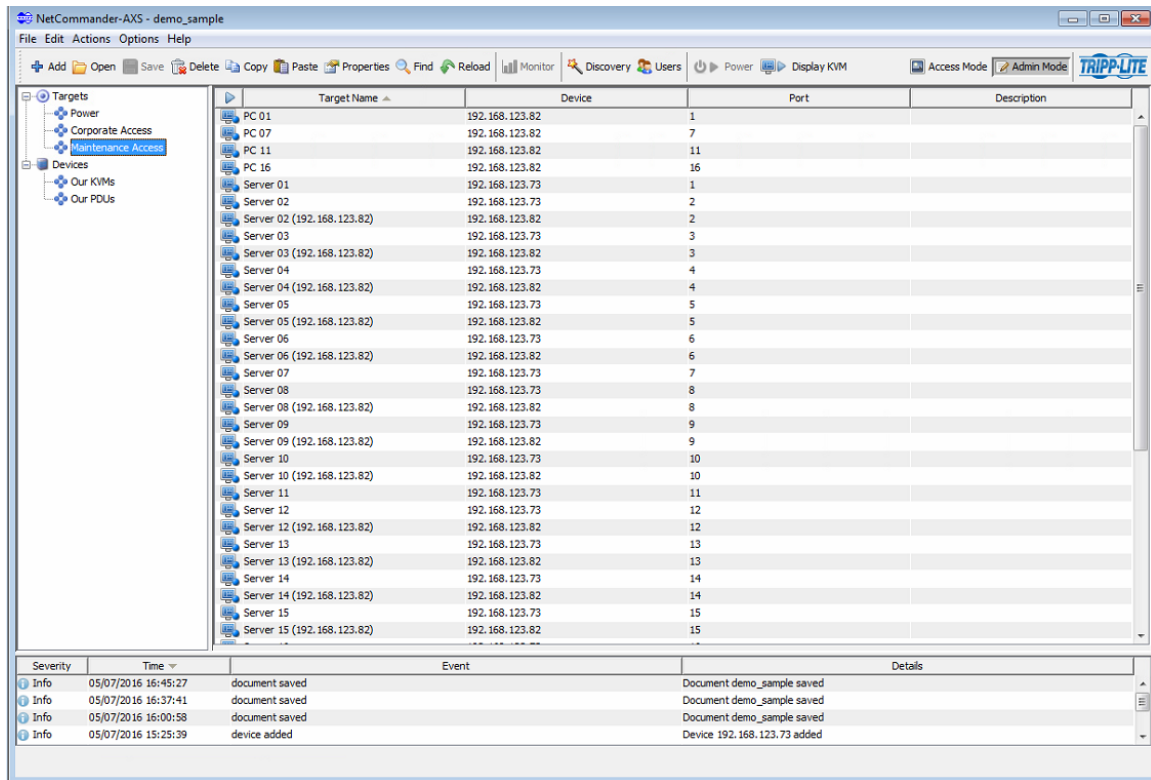
NetCommander-AXS - demo\_sample

File Edit Actions Options Help

Add Open Save Delete Copy Paste Properties Find Reload Monitor Discovery Users Power Display KVM Access Mode Admin Mode TRIPP-LITE

Target Name	Device	Port	Description
Aerospace	192.168.123.88	7	
Audmars Piguet Royal Oak	192.168.123.88	15	
Chronomat	192.168.123.88	9	
Constellation	192.168.123.88	6	
Deville	192.168.123.88	3	
IWC Schaffhausen	192.168.123.88	13	
Navitimer	192.168.123.88	10	
PloProof	192.168.123.88	5	
Rolex Submariner	192.168.123.88	14	
SeaMaster	192.168.123.88	2	
SeaMaster Planet Ocean	192.168.123.88	4	
Seiko Tuna	192.168.123.88	11	
Speedmaster	192.168.123.88	1	
Superocean	192.168.123.88	8	
Ulysse Nardin	192.168.123.88	16	
Zenith El Primero	192.168.123.88	12	

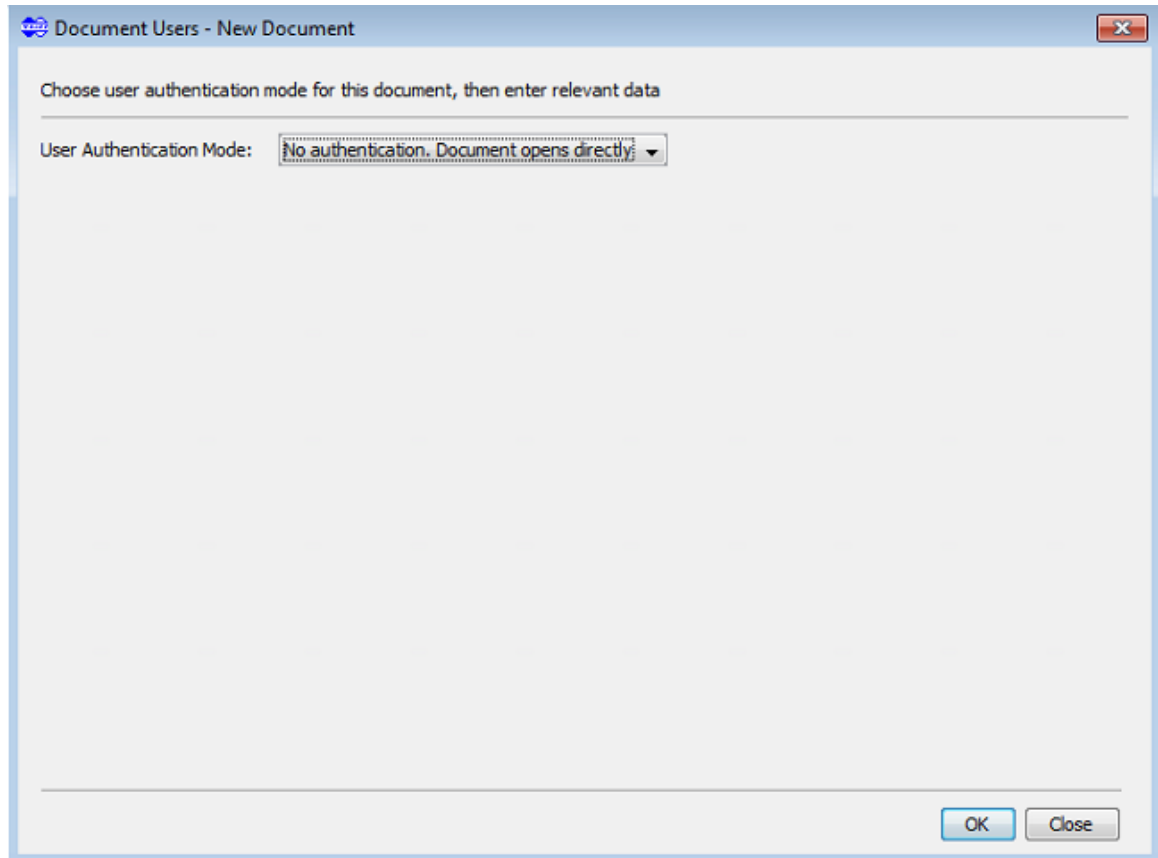
Severity	Time	Event	Details
Info	05/07/2016 16:45:27	document saved	Document demo_sample saved
Info	05/07/2016 16:37:41	document saved	Document demo_sample saved
Info	05/07/2016 16:00:58	document saved	Document demo_sample saved
Info	05/07/2016 15:25:39	device added	Device 192.168.123.73 added



## Saving Your Document

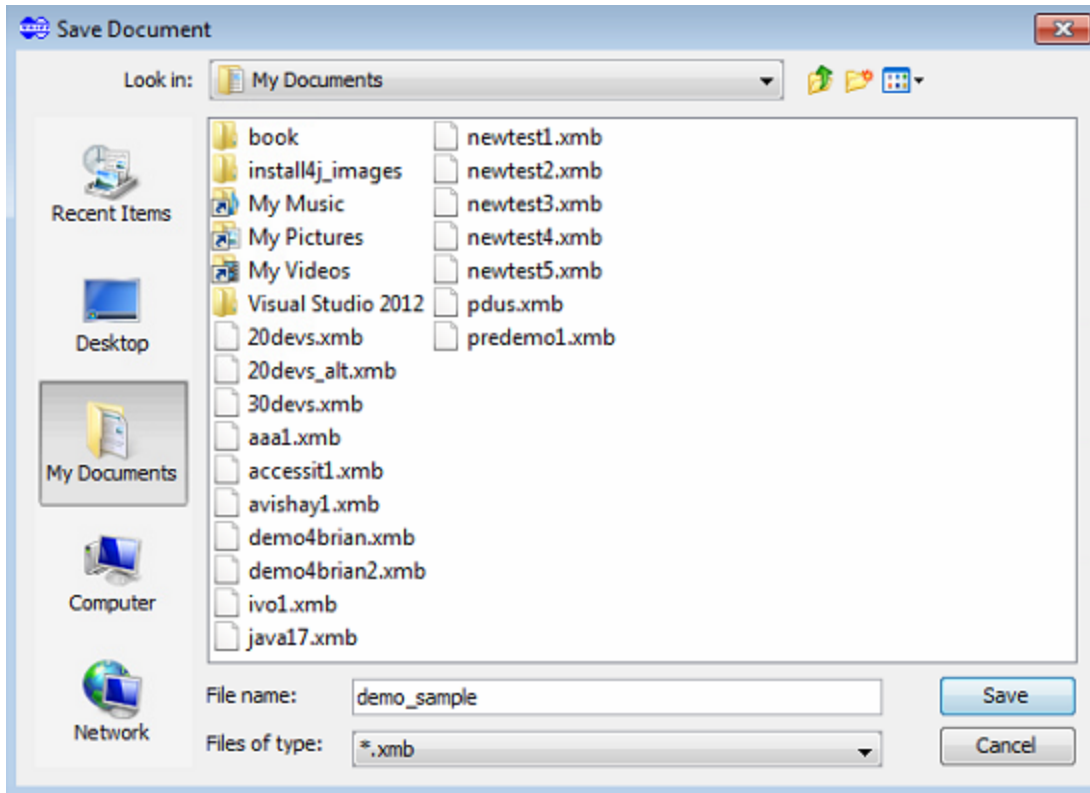
Preserve and persist the data in this 'Getting Started' session for now by saving it in a document to file. The 'document' is an encrypted file that represents the resources we have. As with file management in general, you can create any versions of documents you want, which can be subsequently loaded on demand.

- Select the Save toolbar button
- You are prompted with the Document Users dialog. For this example, simply select 'OK' to indicate no authentication for this document. (Other authentication options are discussed in greater detail in later sections.) Dialog image is shown below:



- You are then prompted to supply a document file name and location. Provide a meaningful name and location, let's say 'demo\_sample', then select 'Save'. An example of this is shown in the image below:





## Access Mode and Admin Mode

The NetCommander-AXS is always running in one of two modes:

### Admin Mode

Admin mode is the mode that allows the user to edit the Document being rendered. The demo example explained up until now has been running in admin mode.

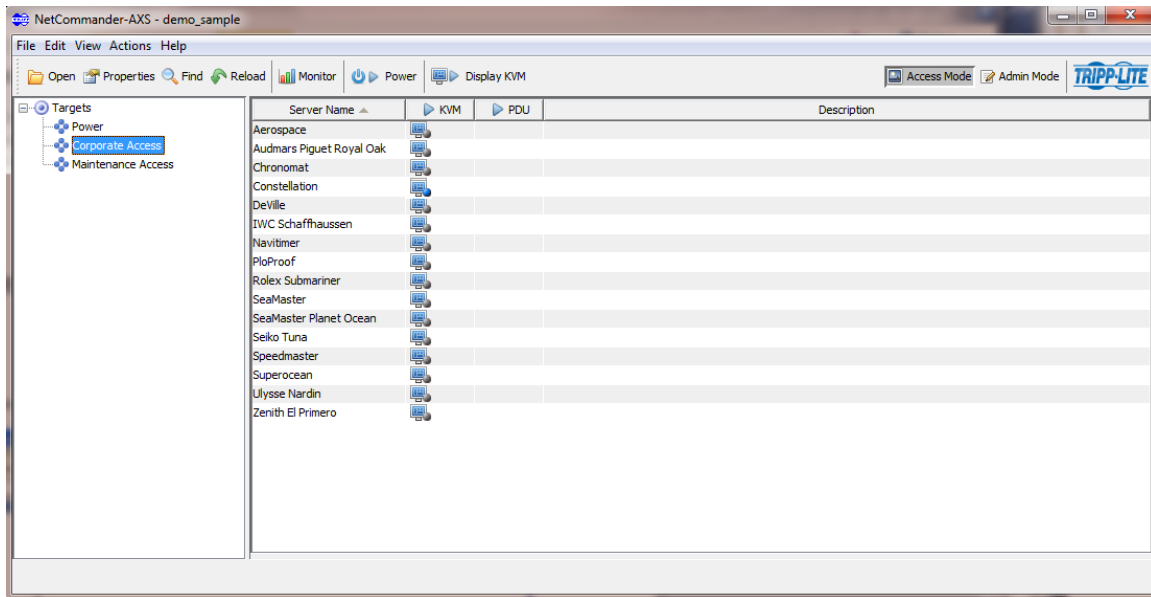
### Access Mode

Display mode is the mode allowing the user to display KVM targets and/or display & manipulate PDU outlets. This mode is not editable. When starting the NetCommander-AXS, it enters Access Mode. The user can toggle between Admin mode and Access mode via the Access Mode / Display Mode toggle button in the toolbar. Note that the user can display KVM targets and/or manipulate PDU outlets through the Admin Mode as well.

### Display KVM Targets

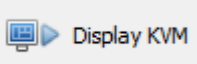
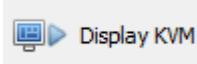
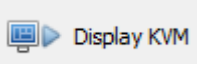
With discovered KVM devices and targets now saved in the document, close the NetCommander-AXS, and reenter it through the Windows Start->Programs-> Tripp Lite NetCommander-AXS menu.

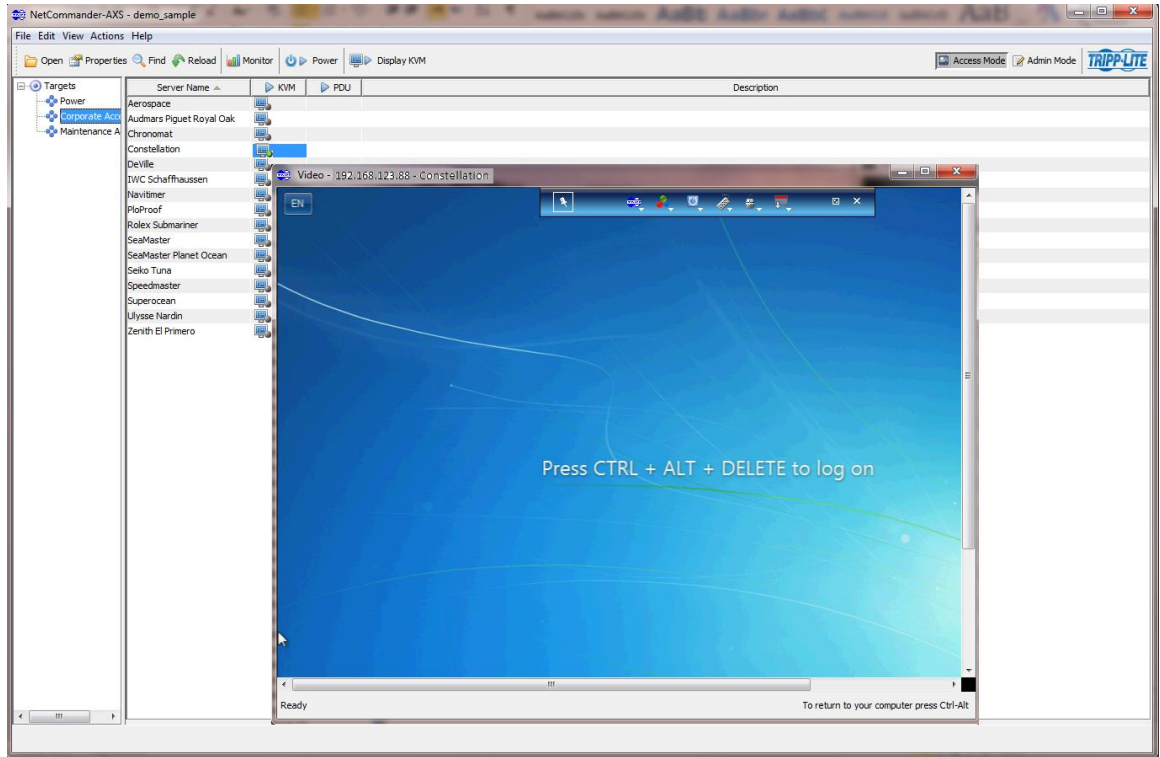
Select the Corporate Access group in the groups tree. The view should be similar to:



Actual display of KVM video display for selected targets is now possible.

To display a KVM video display:

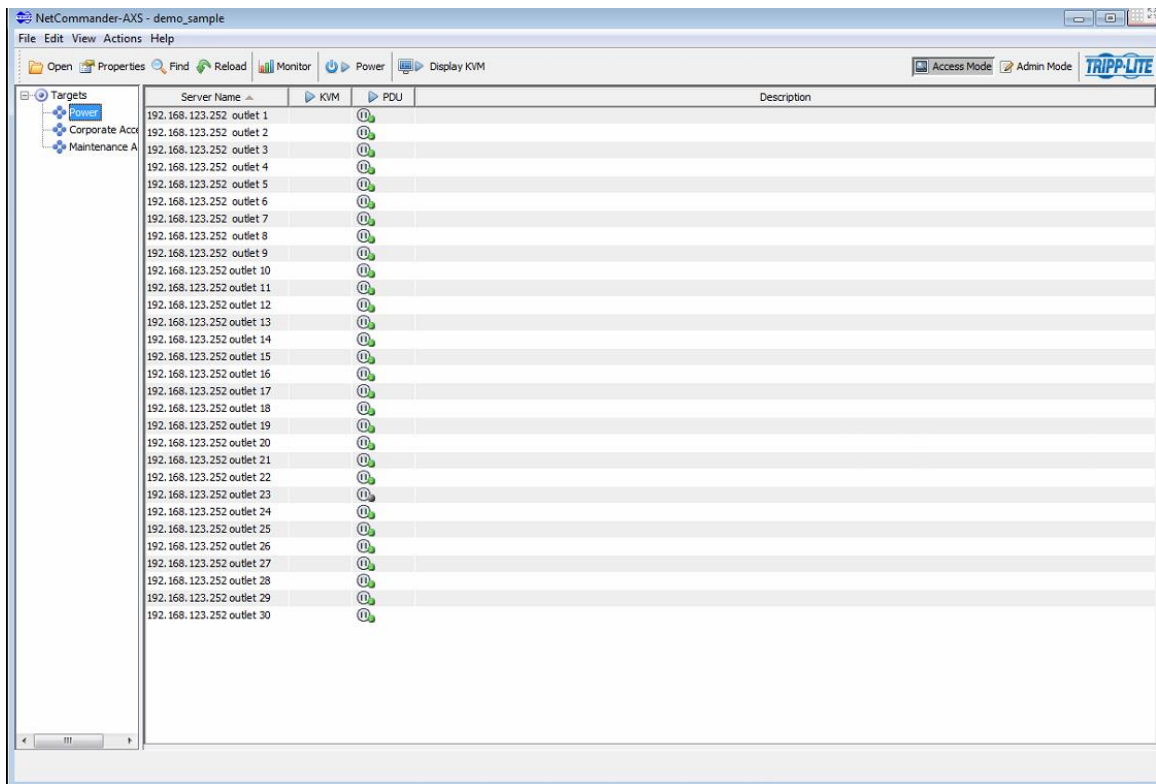
- Double-click the cell of interest under the KVM column, or ,
- Select the cell of interest and either:
  - Select the 'Display KVM' button in main toolbar [  ]
  - Right-click and pick the  popup menu item
  - Pick the main menu Actions->  menu item
- Below is an example of displaying KVM video for target "Constellation" in our example.



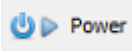

At this point, you can continue and display any other targets you desire.

## Manipulate PDU Target States

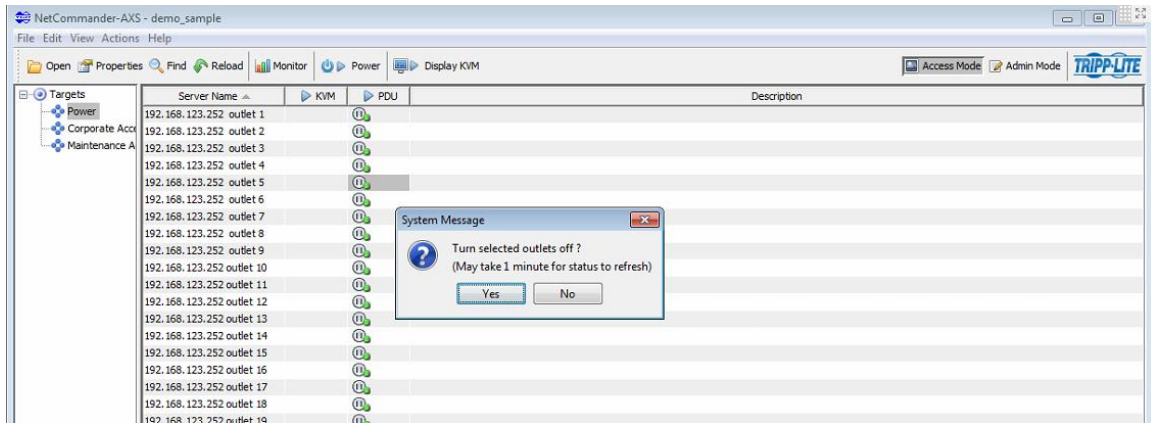
Select the Power group in the groups tree. The view should be similar to:



To manipulate a PDU outlet, or outlets:

- Select the PDU target cell of interest (or several cells) and either:
  - Right-click and select the Power popup menu and then one of “On”, “Off”, “Cycle”, or “Status”
  - Pick the main toolbar “Power” button , and then one of “On”, “Off”, “Cycle”, or “Status” menu items
  - Pick the main menu Actions->  menu, and then one of “On”, “Off”, “Cycle”, or “Status” menu items

For each of the above (except Status), you will be prompted to confirm the desired activity, with a note that the status may take a minute to refresh. Example:



## Reloading Your Document

- If you close the NetCom Commander-AXS application, and reopen it, the last saved document will be reloaded by default.
- Should you create and save several documents you can load them on demand through the File->Open... menu.

This completes the Quick Start section. The remainder of this documentation provides further details on major concepts of the NetCom Commander-AXS.

## NetCom Commander-AXS Window

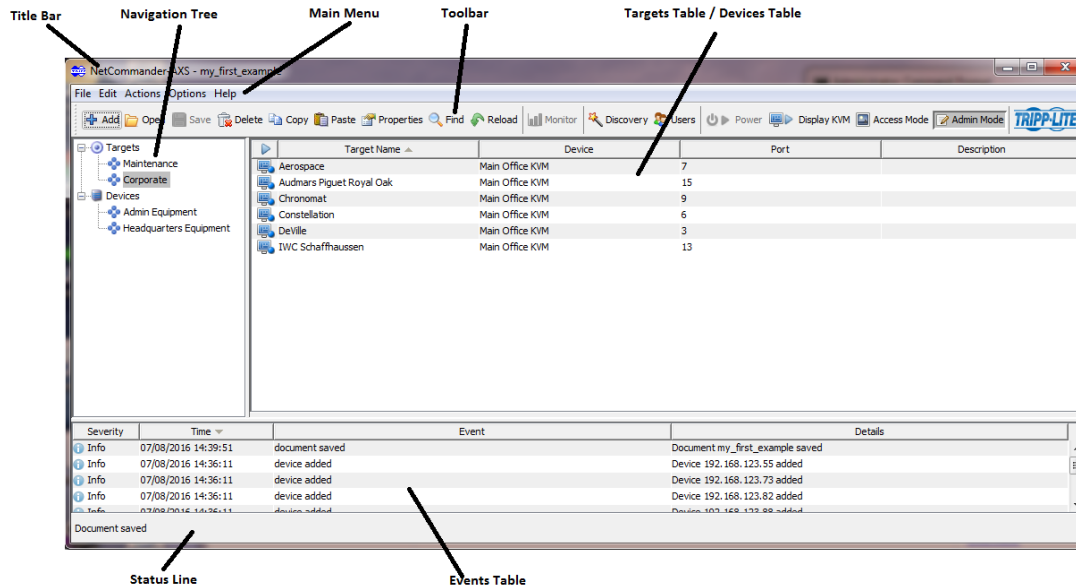
The NetCom Commander-AXS application runs with a single main window.

### Window Components

Main areas of the screen include:

- Title bar. Indicates name of Document being edited
- Main menu. Standard application window menu
- Toolbar. Standard application toolbar.
- Navigation Tree. Selecting within the Navigation tree loads the relevant Target or Device Group into the corresponding Targets Table or Devices Table.
- Devices Table. Details a list of defined Devices within the selected Group for the given Document
- Targets Table. Details a list of defined Targets within the selected Group for the given Document
- Events Table. Lists events that have occurred within NetCom Commander-AXS activity.

An image of the NetCom Commander-AXS Window with indications of its areas is shown below:



## Convenience Features

The NetCommander-AXS provides:

- Copy-paste of Targets and Devices
- Drag-drop of Devices and Targets to different Groups

## Managed Elements

### Document

The NetCommander-AXS Document element represents a set of definitions of:

- KVM and PDU Devices
- KVM and PDU Targets
- Groups of Devices and Targets

The NetCommander-AXS Window opens and presents a Document for viewing and editing (if in admin mode). Through a document, a KVM target is selected and displayed in a separate video window. A PDU target is displayed with its status as well as the ability to turn it on, off, or cycle.

Documents are actual files in a Microsoft Windows directory. The name in the title bar of the NetCommander-AXS Window is the same as the Document's file name. The files are of a proprietary extension .xmb, and its contents are encrypted.

A Document will have one of several authentication modes through which a user accesses the Document. See discussion in the User Authentication section.

## Group

Groups contain Device or Target definitions. Every Device and Target definition has an associated Group.

The root Group for Targets is called "Targets". The root Group for Devices is called "Devices". These 2 Groups are always displayed in the navigation tree.

## Adding a Group

In Admin mode, Groups can be added under the root groups.

To add a Devices Group, select the "Devices" Group and pick Add Group through

- Popup menu
- Main menu
- Toolbar

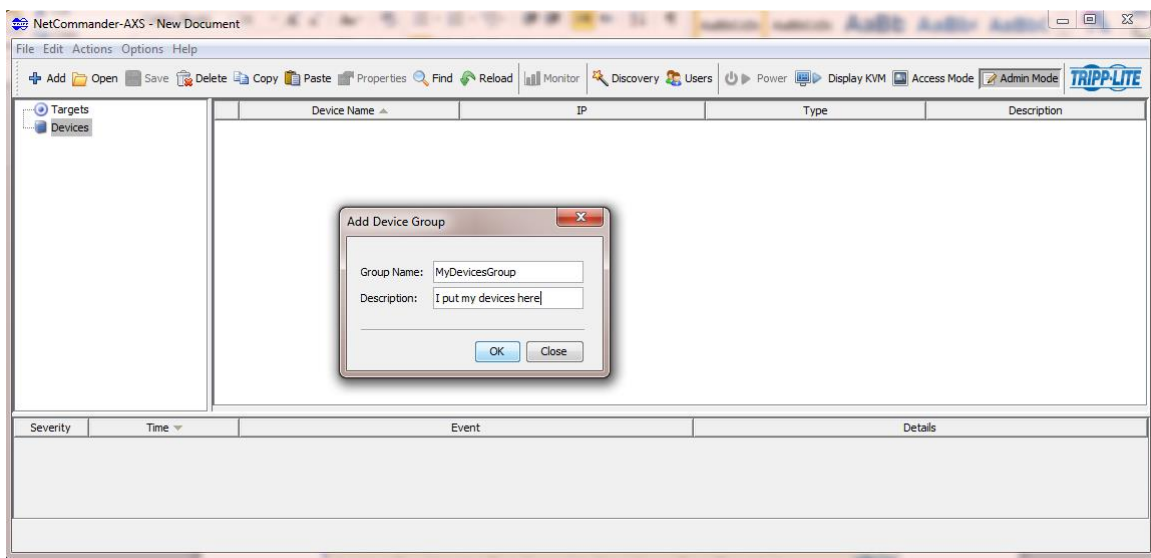
A new Device Group can be added under the Devices Groups only.

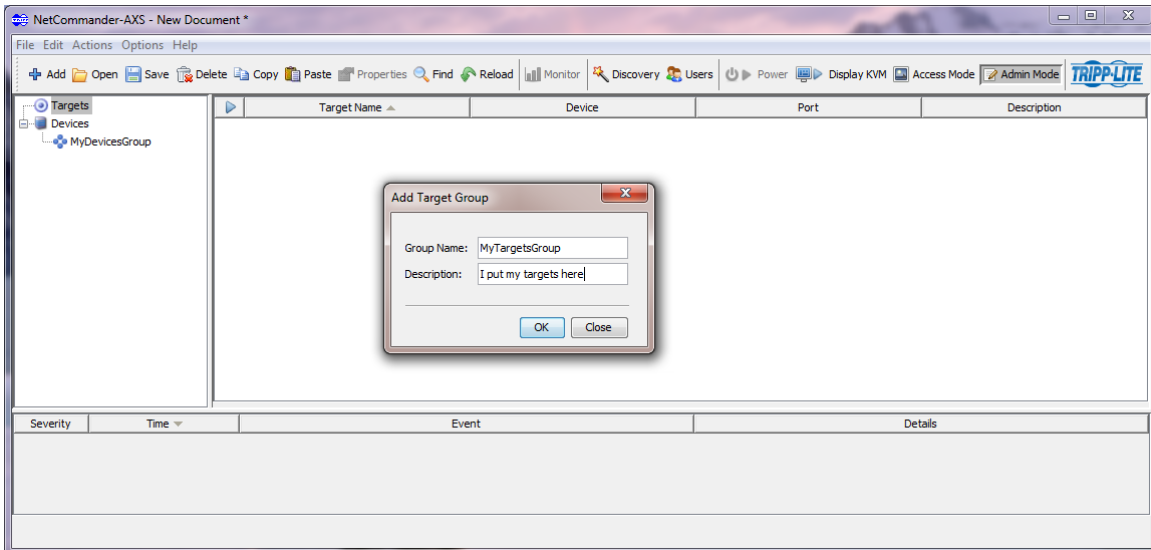
To add a Targets Group, select the "Targets" Group and pick Add Group through

- Popup menu
- Main menu
- Toolbar

A new Target Group can be added under the Targets Groups only.

Fill out the resulting dialog and select OK. See example images below:





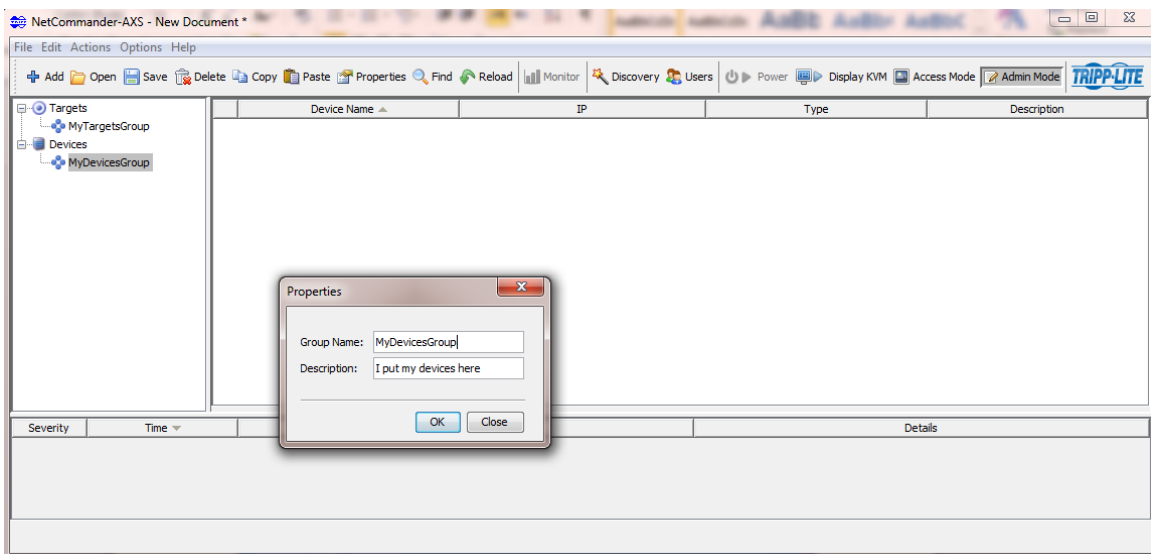
## Editing a Group

In Admin Mode, to edit a non-root Group, select the Group of interest, and select “Properties” with either

- Popup menu
- Main menu
- Toolbar

Edit the group name and/or description in the Properties dialog, then select OK.

See example below for a Device Group:





## Deleting a Group

In Admin Mode, A non-root Group can be deleted by selecting it and selecting Delete through:

- Popup menu
- Main menu
- Toolbar
- Selecting the Delete key

The group will be deleted, including any relevant Devices and Targets

## KVM and PDU Devices

A Device definition represents either a Tripp Lite KVM or PDU Device. Devices are added either through discovery (see Discovery section) or manually, as described in this section. A KVM Target definition has an associated KVM Device definition. Likewise a PDU Target definition has an associated PDU Device definition

## Adding a KVM Device

In Admin Mode, make sure the Devices table is showing by selecting a Device Group of interest in the NetCommander-AXS Window. Then select “Add KVM Device” through:

- Popup menu
- Main menu
- Toolbar

The Add KVM Device dialog is then displayed. Below are 2 images of this dialog.

- Device Tab of Add KVM Device dialog:

Add KVM Device X

Device **Targets**

Device Name:

Device Type: Tripp Lite 4x32 KVM ▼

IP:

TCP Port:

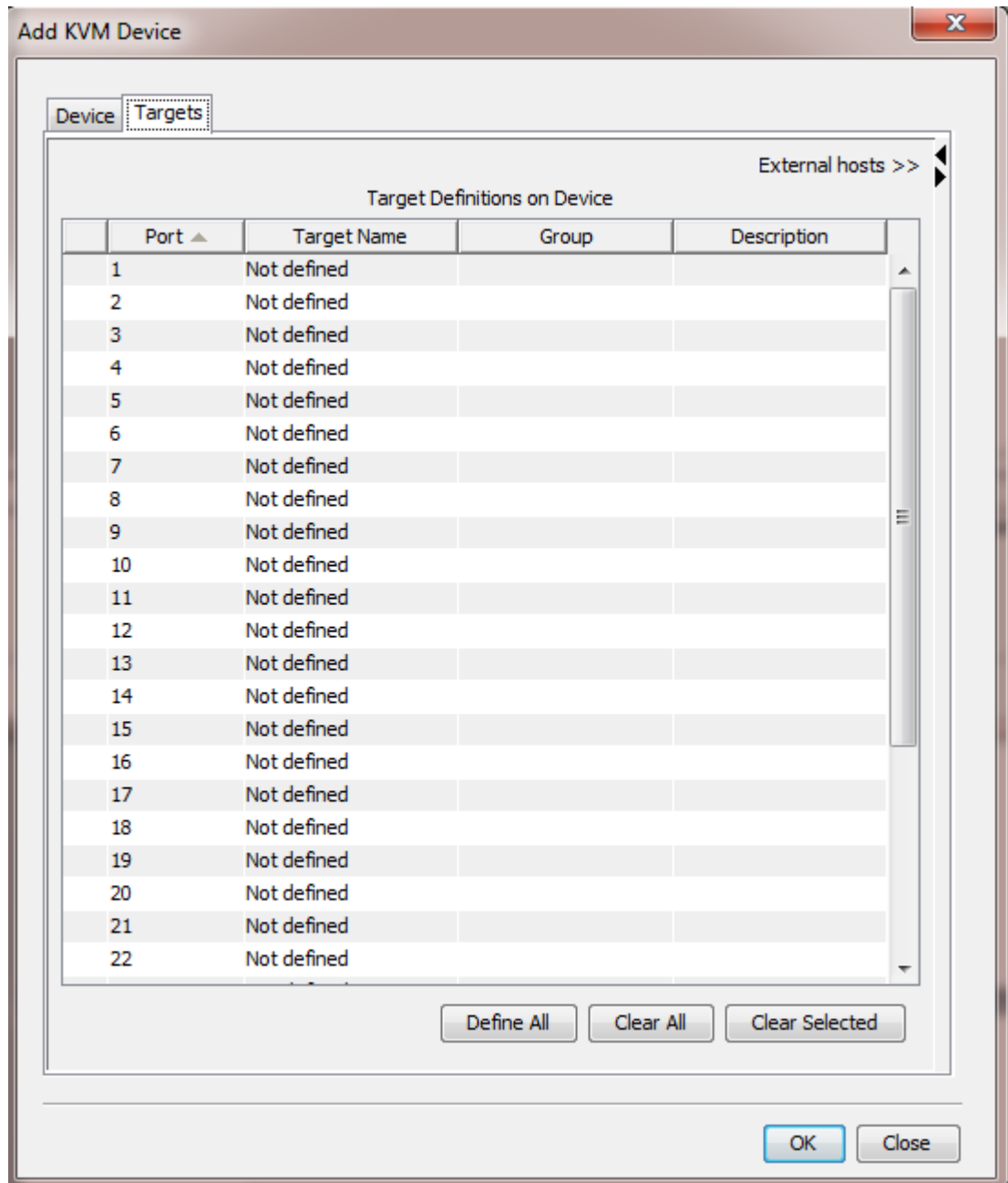
Login Name:

Password:

Confirm Password:

Description:

- Targets Tab of KVM Device dialog:



Fill out the required fields of

- Device name
- Device type
- IP address
- TCP port
- Device login name
- Device password

You can optionally fill out:

- Description
- Targets. You can manually define individual Targets with distinct names and Target Group locations. For any Target names left not defined, upon Oking the dialog, the software will attempt to access the device and initialize target names based on the names as indicated on the device itself.

Select OK to commit the dialog's definitions to the NetCommander-AXS window.

## **Adding a PDU Device**

In Admin Mode, make sure the Devices table is showing by selecting a Device Group of interest in the NetCommander-AXS Window. Then select "Add PDU Device" through:

- Popup menu
- Main menu
- Toolbar

The Add PDU Device dialog is then displayed. Below are 2 images of this dialog.

- Device Tab of Add PDU Device dialog:

Add PDU Device

Device | SNMP | Targets

Device Name:

Device Type: Tripp Lite 30 Port PDU (PDU3VSR.2) ▼

Manufacturer: Tripp Lite

IP:

Description:

OK Close

- SNMP Tab of PDU Device dialog:

Add PDU Device

Device SNMP Targets

Protocol: SNMP v1

SNMP Port (0-65535): 161

Retries (0-10): 2

Timeout Period (1-300 secs): 5

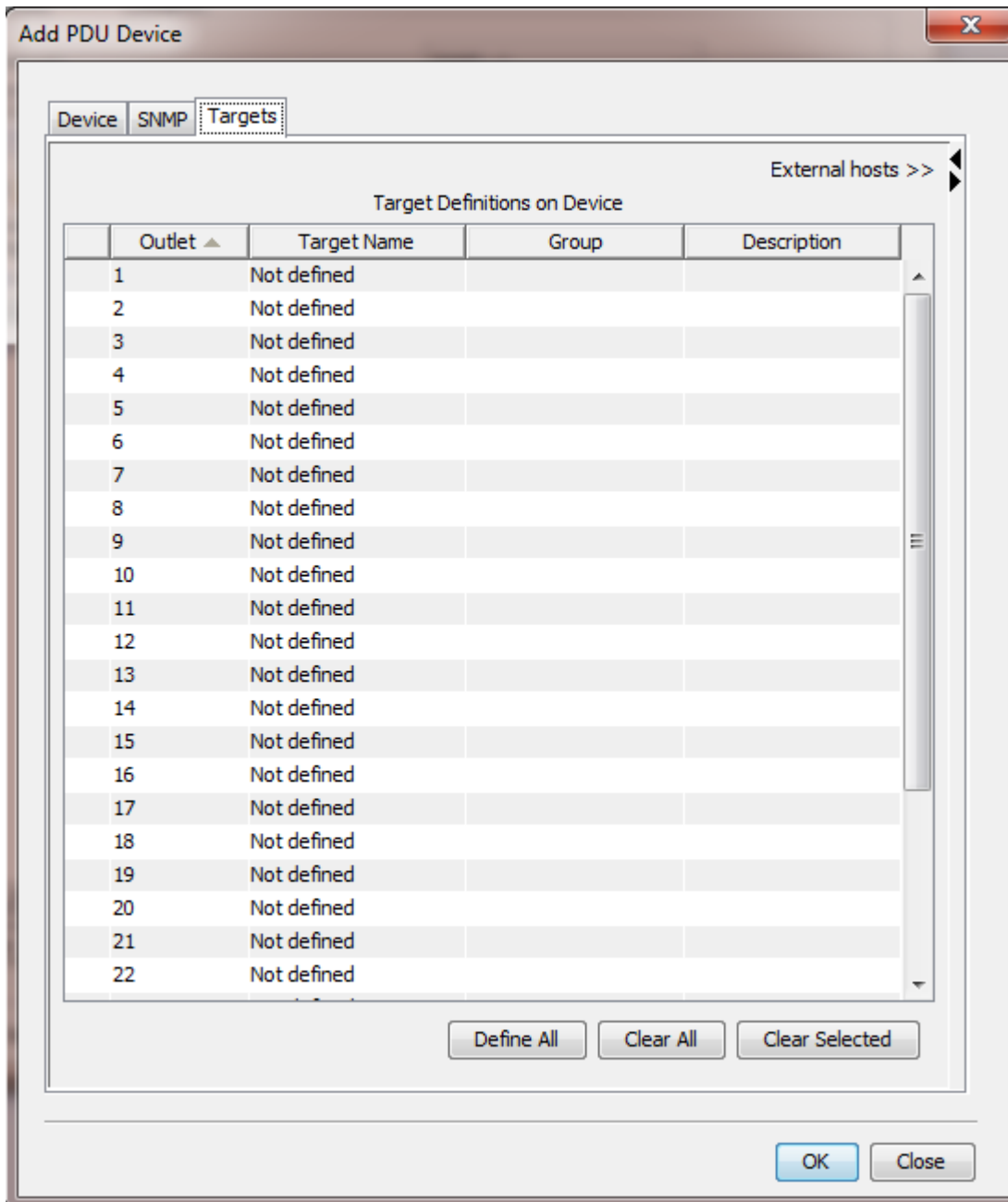
Read Community: public

Write Community:

Confirm Write Community:

OK Close

- Targets Tab of PDU Device dialog:



Fill out the required fields of

- Device name
- Device type
- IP address
- SNMP protocol
- SNMP port
- SNMP retries
- SNMP timeout period

- SNMP read and write community

You can optionally fill out:

- Description
- Targets. You can manually define individual Targets with distinct names and Target Group locations. For any Target names left not defined, upon Oking the dialog, the software will attempt to access the device and initialize target names based on the names as indicated on the device itself.

Select OK to commit the dialog's definitions to the NetCommander-AXS window.

## Editing a Device

In Admin Mode, to edit a Device, select the Device of interest in the Devices table in the NetCommander-AXS Window. Then select "Properties" through:

- Popup menu
- Main menu
- Toolbar

The Device Properties dialog is displayed, and initialized with the Device's data. The dialog components are similar to those in the Add Device section.

Upon selecting the OK button, the Device's attributes are updated in the NetCommander-AXS Window.

Additionally, some attributes of a Device can be edited directly with in-place Device table editing. Attributes include Device name, IP address, and description.

## Deleting Devices

In Admin mode, to delete Devices, select the Devices to be deleted in the Devices table in the NetCommander-AXS Window and then selecting Delete through:

- Popup menu
- Main menu
- Toolbar
- Selecting the Delete key

The Devices will be deleted, including any relevant Targets



## KVM and PDU Target

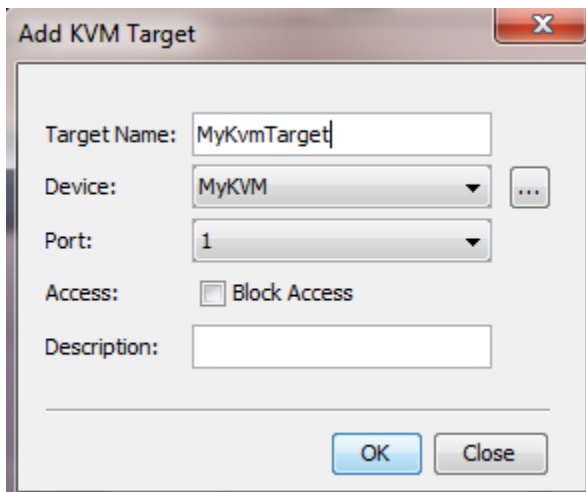
A Target definition, for a KVM, represents a port on a KVM Device through which a KVM video window is opened. For a PDU, a Target represents an outlet on a PDU device. Targets are added either through Discovery (see Discovery section), by default when adding a device as described in this section, or directly in manual fashion, as described here. A KVM Target definition has an associated KVM Device definition, and a PDU Target definition has an associated PDU Device definition.

### Adding a KVM Target

In Admin Mode, make sure the Targets table is showing by selecting a Target Group of interest in the NetCommander-AXS Window. Then select “Add KVM Target” through:

- Popup menu
- Main menu
- Toolbar

The Add KVM Target dialog is then displayed. Below is an image of this dialog.



Fill out the required fields of

- Target name
- KVM Device associated with target
- Target port

You can optionally fill out:

- Select 'Block Access' to prevent access to the target
- Description

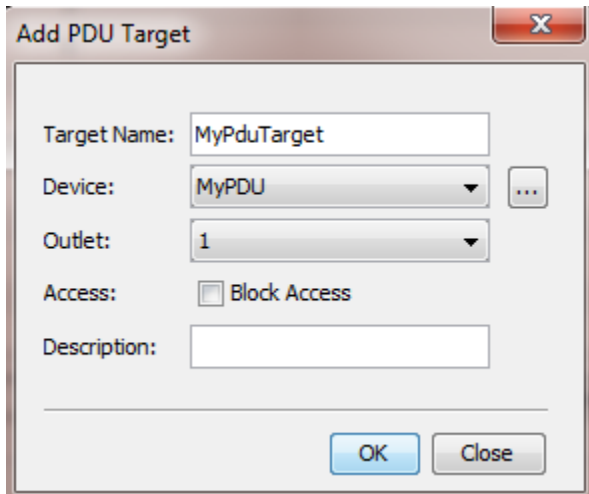
Select OK to commit the dialog's definitions to the NetCommander-AXS window.

## Adding a PDU Target

In Admin Mode, make sure the Targets table is showing by selecting a Target Group of interest in the NetCommander-AXS Window. Then select “Add PDU Target” through:

- Popup menu
- Main menu
- Toolbar

The Add PDU Target dialog is then displayed. Below is an image of this dialog.



Fill out the required fields of

- Target name
- PDU Device associated with target
- Target outlet

You can optionally fill out:

- Select ‘Block Access’ to prevent access to the target
- Description

Select OK to commit the dialog’s definitions to the NetCommander-AXS window.

## Editing a Target

In Admin Mode, to edit a Target, select the Target of interest in the Targets table in the NetCommander-AXS Window. Then select “Properties” through:

- Popup menu
- Main menu
- Toolbar

The Target Properties dialog is displayed, and initialized with the Target's data. The dialog components are similar to those in the Add Target section.

Upon selecting the OK button, the Target's attributes are updated in the NetCommander-AXS Window.

Additionally, some attributes of a Target can be edited directly with in-place Target table editing. Attributes include Target name, Target's Device, port number, and description

## Deleting Targets

In Admin Mode, to delete Targets, select the Targets to be deleted in the Targets table in the NetCommander-AXS Window and then selecting Delete through:

- Popup menu
- Main menu
- Toolbar
- Selecting the Delete key

The Targets will be deleted.

## External Hosts

External Hosts refers to using lists of host details for assigning to Target names. Typically, a user will want to assign meaningful names to targets which can be found in these external host lists. There are 3 types of external hosts sources:

- Text File
- LDAP
- DNS

External hosts are used in:

- Targets tab in the Add Device dialog
- Targets tab in the Edit Device dialog
- Discovery Results dialog

The user can easily drag-and-drop host details into Target definitions.

## Defining External Hosts Source

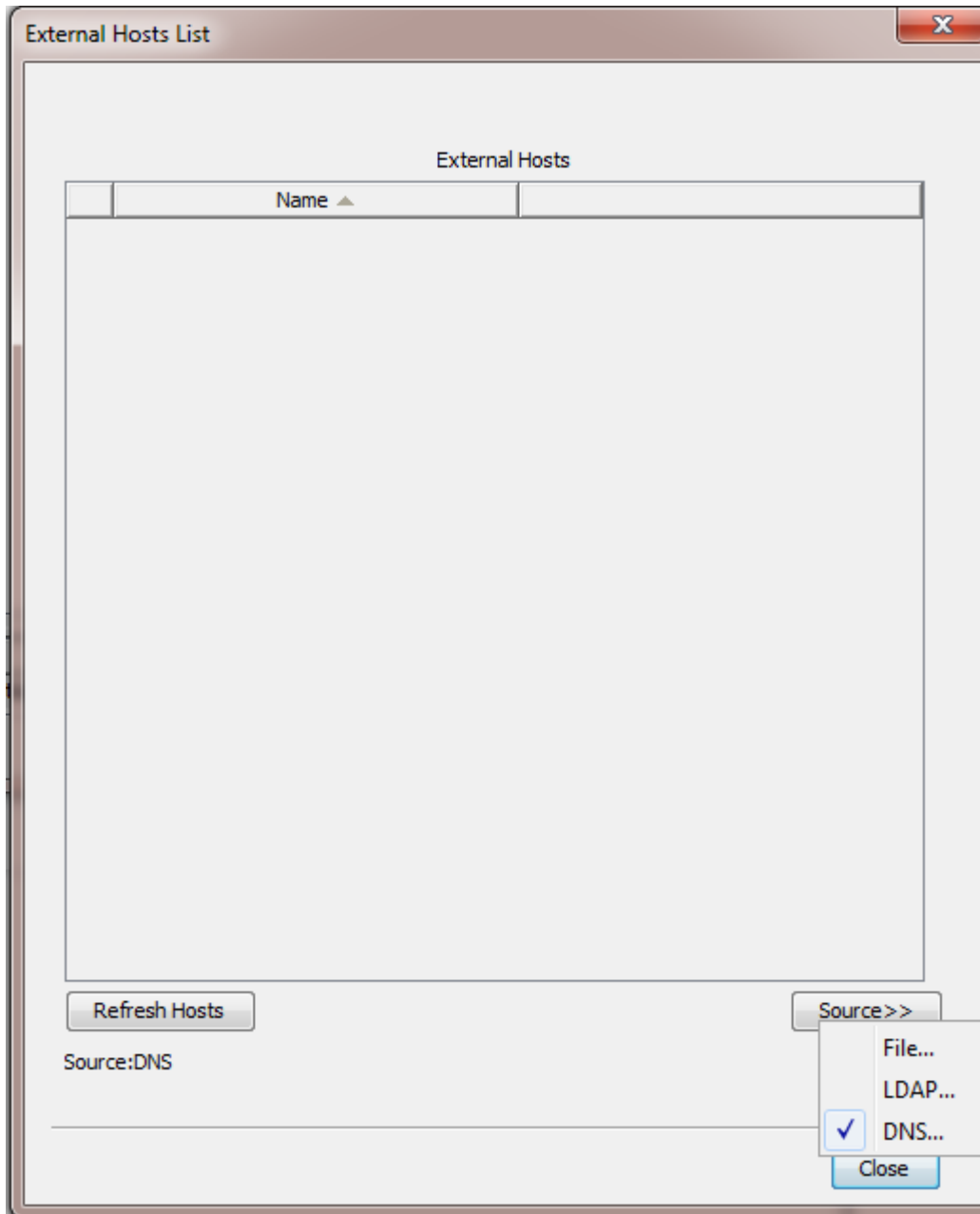
Defining of an External Hosts Source is done through selecting either:

- Selecting the "Source>>" button in the dialog resulting from selecting File->External Hosts List menu item

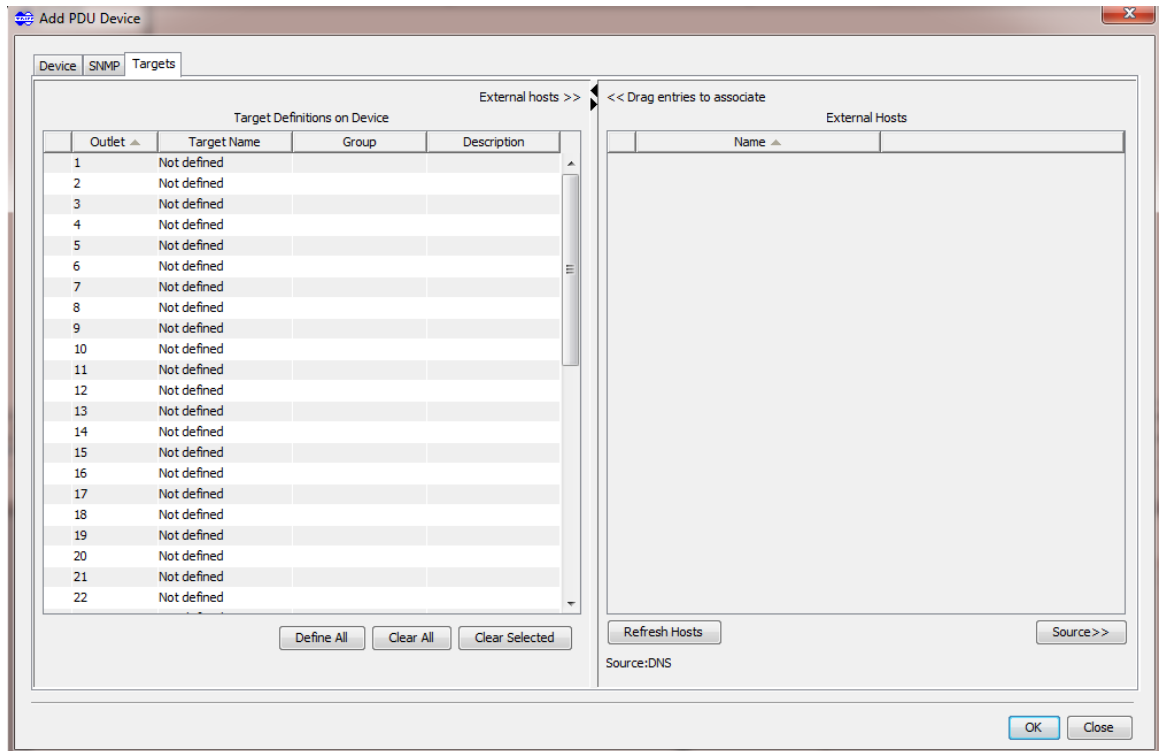
- “Source>>” button in the expanded split pane within the Targets tab in the Add Device or Edit Device dialog
- Filling out the Hosts tab in the Discovery dialog

Image of selecting the “Source>>” button for each of the above is shown below is shown below:

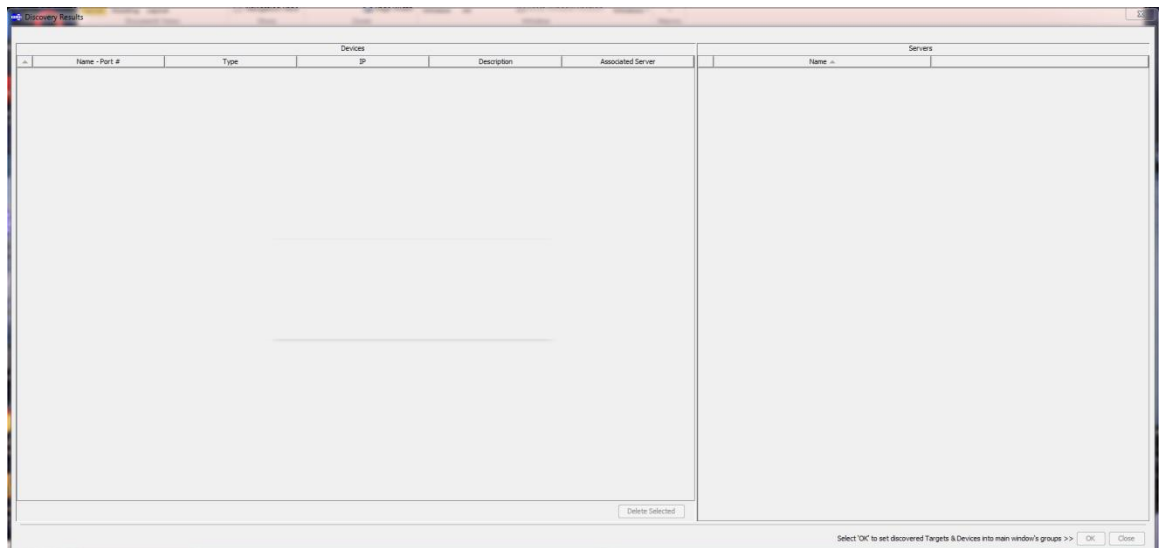
- External Hosts List:



- Device dialog expanded Targets tab:



External hosts in discovery dialog (right-side):



## File-based External Hosts

Selecting the "File..." menu item in both cases above will show a file manager dialog, prompting the user to select a .csv file.

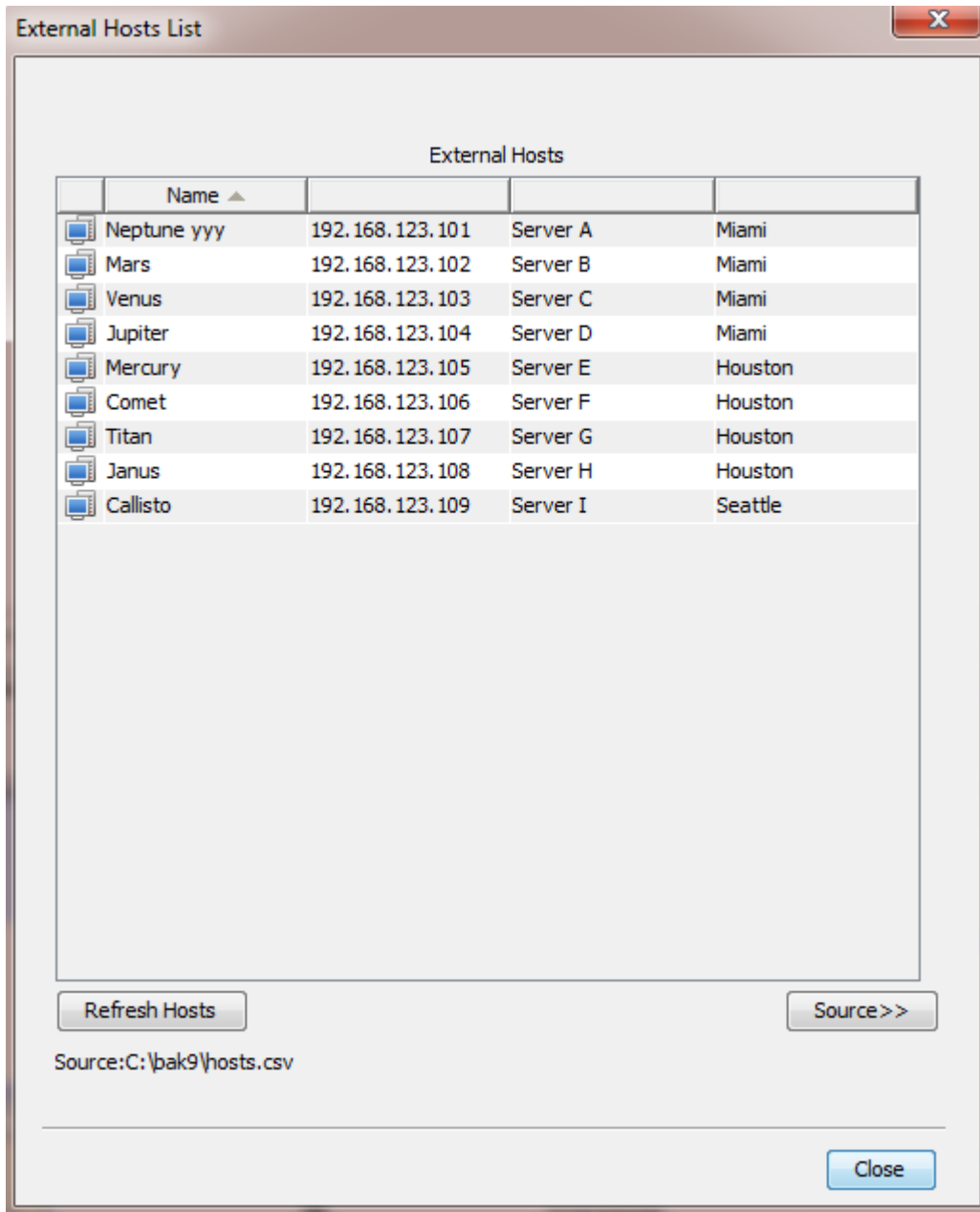
The expected syntax of the .csv file:

- First row is column titles
- Subsequent rows are comma-delimited entries such that the first entry in each row is the host name, and anything else is considered descriptive information.

## File-based External Hosts Configuration Example

Below is an image of an external host list shown in the dialog. Below it are the first few lines of the file that it is displaying.

- Dialog Example:

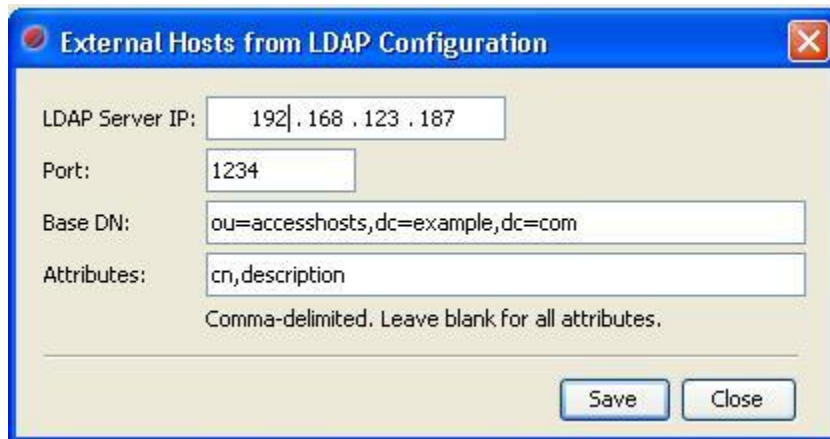


- File Content for Above Example:

Host,IP,Tag,Location  
Neptune yyy,192.168.123.101,Server A,Miami  
Mars,192.168.123.102,Server B,Miami  
Venus,192.168.123.103,Server C,Miami  
Jupiter,192.168.123.104,Server D,Miami  
Mercury,192.168.123.105,Server E,Houston  
Comet,192.168.123.106,Server F,Houston  
Titan,192.168.123.107,Server G,Houston  
Janus,192.168.123.108,Server H,Houston  
Callisto,192.168.123.109,Server I,Seattle  
...

## LDAP-based External Hosts

Selecting the “LDAP...” menu item in both cases above will show an LDAP configuration dialog, prompting the user to enter relevant entries for querying LDAP hosts. Image of the dialog is shown below:



External Hosts from LDAP Configuration

LDAP Server IP: 192.168.123.187

Port: 1234

Base DN: ou=accesshosts,dc=example,dc=com

Attributes: cn,description

Comma-delimited. Leave blank for all attributes.

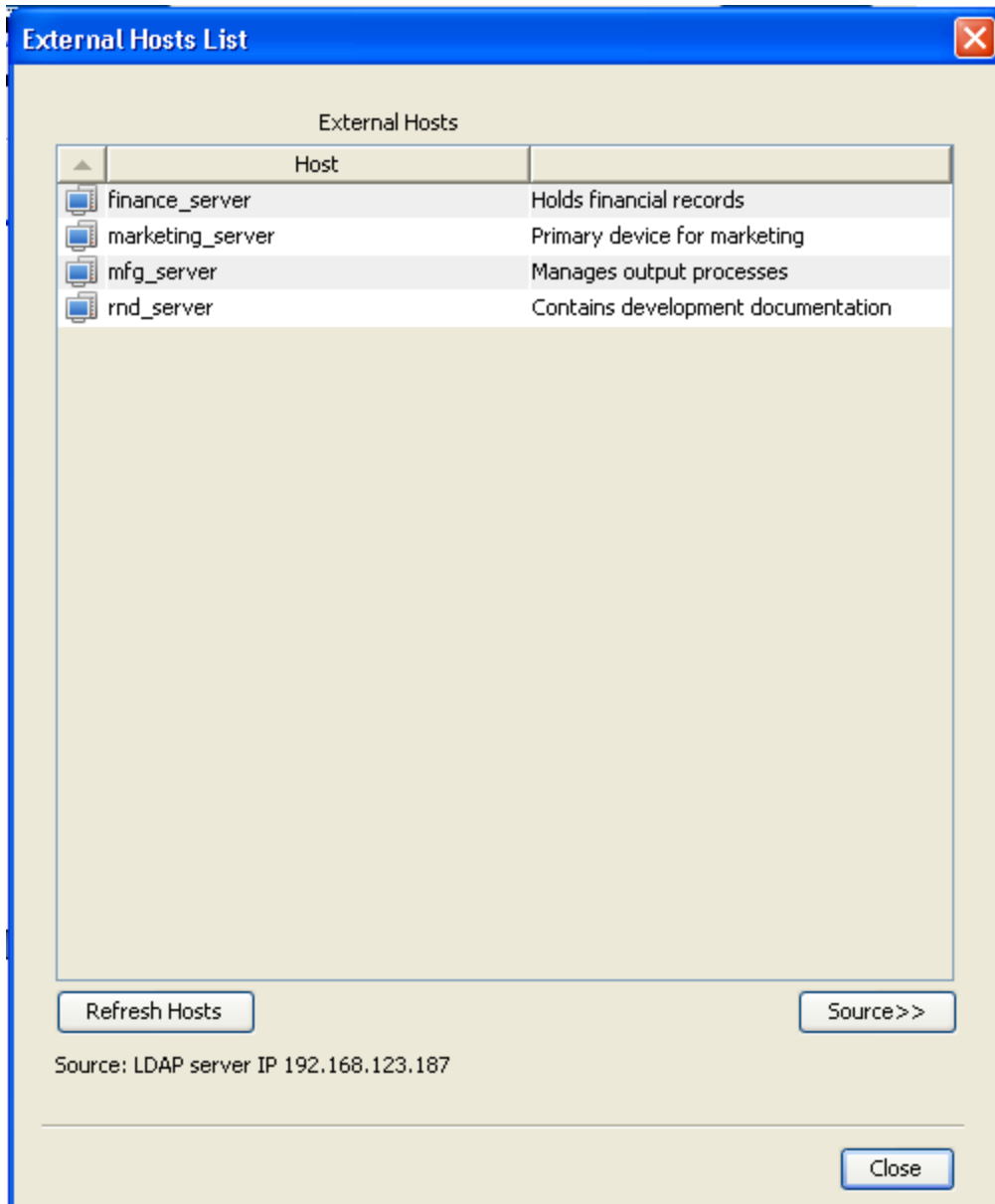
Save Close

User needs to specify:

- LDAP server IP address to query from
- LDAP server port
- Base DN containing the list of hosts
- Attribute(s) to display in result set

## LDAP-based External Hosts Configuration Example

- For the configuration in the image above, the following results are displayed in this trivial example:



- LDAP file syntax possibility for above:  
dn: ou=accesshosts,dc=example,dc=com  
objectclass: organizationalunit  
ou: hosts  
description: access hosts set  
  
dn: cn=marketing\_server,ou=accesshosts,dc=example,dc=com  
objectclass: device  
cn: marketing\_server  
description: Primary device for marketing



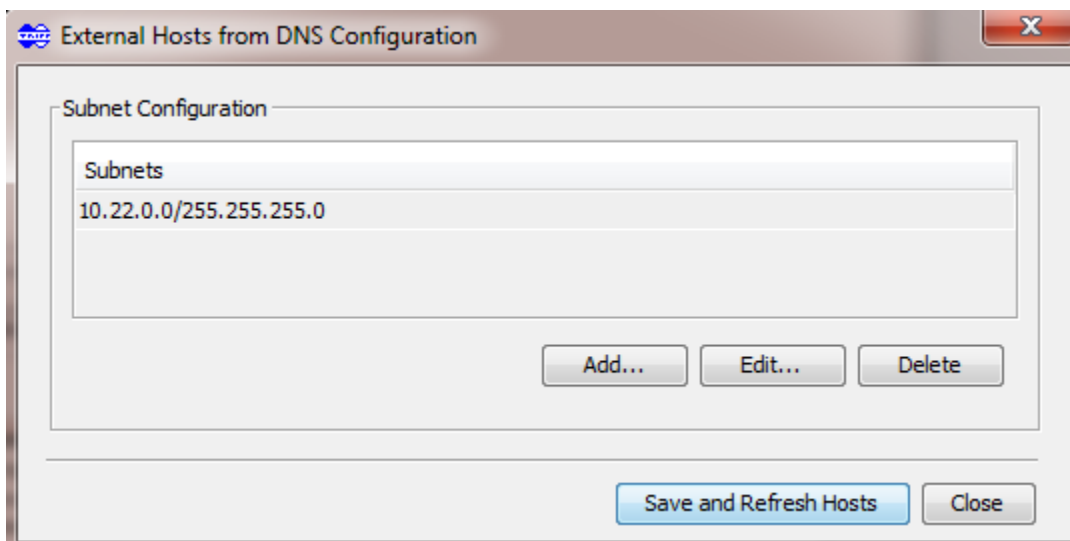
dn: cn=finance\_server,ou=accesshosts,dc=example,dc=com  
objectclass: device  
cn: finance\_server  
description: Holds financial records

dn: cn=rnd\_server,ou=accesshosts,dc=example,dc=com  
objectclass: device  
cn: rnd\_server  
description: Contains development documentation

dn: cn=mfg\_server,ou=accesshosts,dc=example,dc=com  
objectclass: device  
cn: mfg\_server  
description: Manages output processes

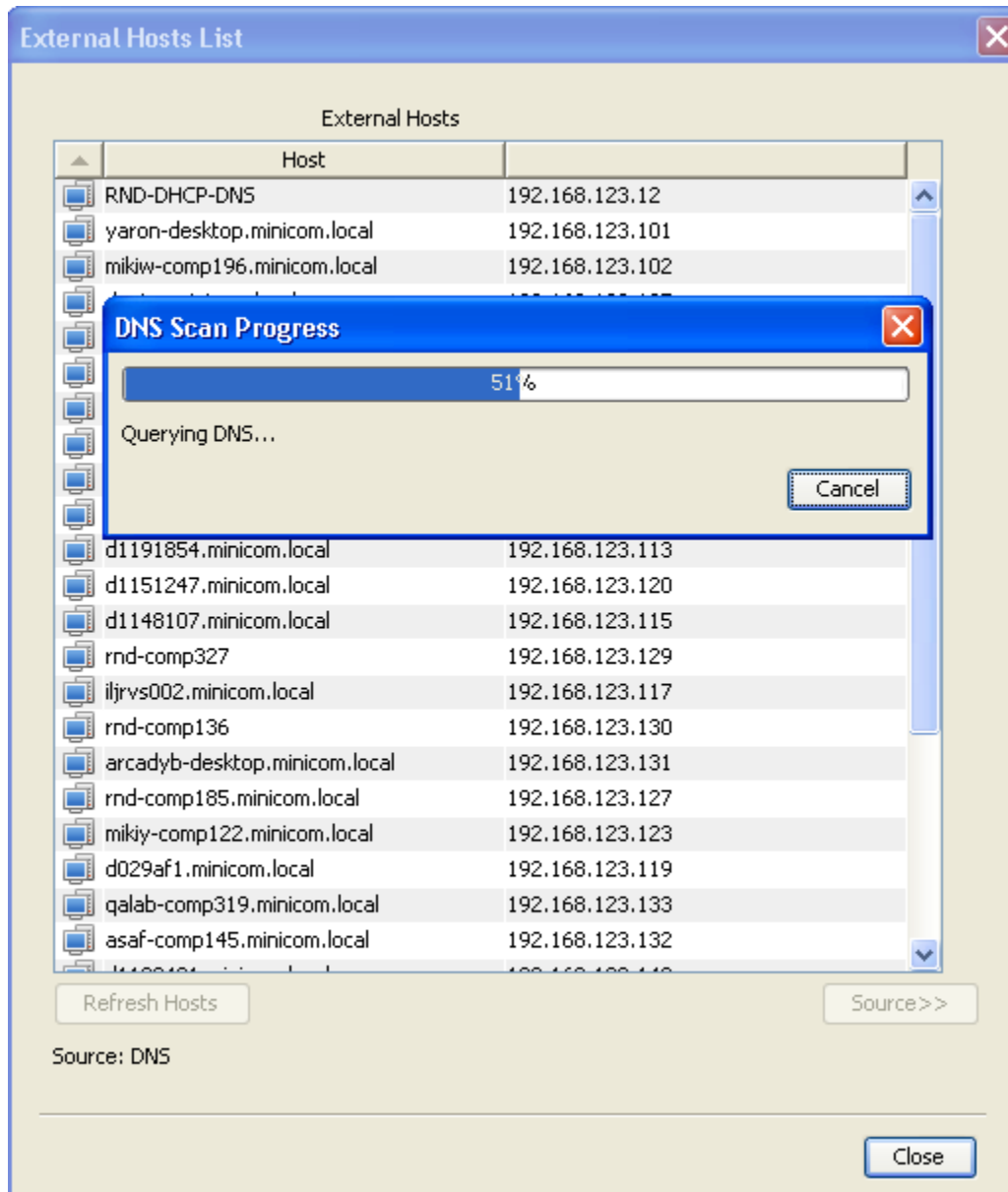
## DNS-based External Hosts

Selecting the “DNS...” menu item will show a DNS configuration dialog, prompting the user to enter relevant subnets over which the DNS entries will be retrieved. Image of the dialog is shown below:



## DNS-based External Hosts Example

For the dialog above, selecting “Save and Refresh Hosts” will fetch the DNS entries on the indicated subnets. Below is a typical response.



## Using External Hosts

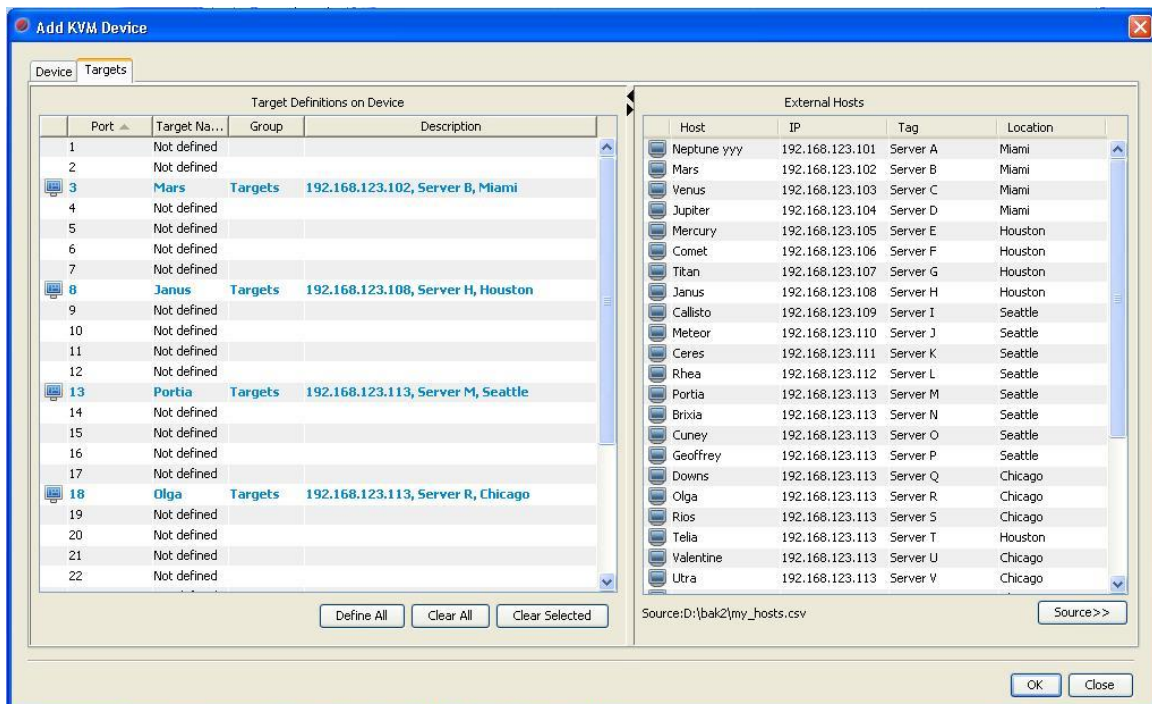
To use external hosts:

- Open an Add Device dialog or Edit Device dialog instance.

- Select Targets tab, and expand right-side splitter
- Drag relevant external hosts onto the associated Targets. Target names and descriptions are updated accordingly.
- See Discovery section and Getting Started section for using external hosts during discovery.

## File-based External Hosts Usage Example

Continuing with the example above, below is an example of opening an Add Device Dialog, and dragging some external host into Targets:



## Device Discovery

The NetCommander-AXS provides functionality to Discover KVM and PDU Devices. Discovered Targets and their associated Devices can then be added into NetCommander-AXS Window

Target Discovery is performed through the Discovery dialog. To show the Discovery dialog either:

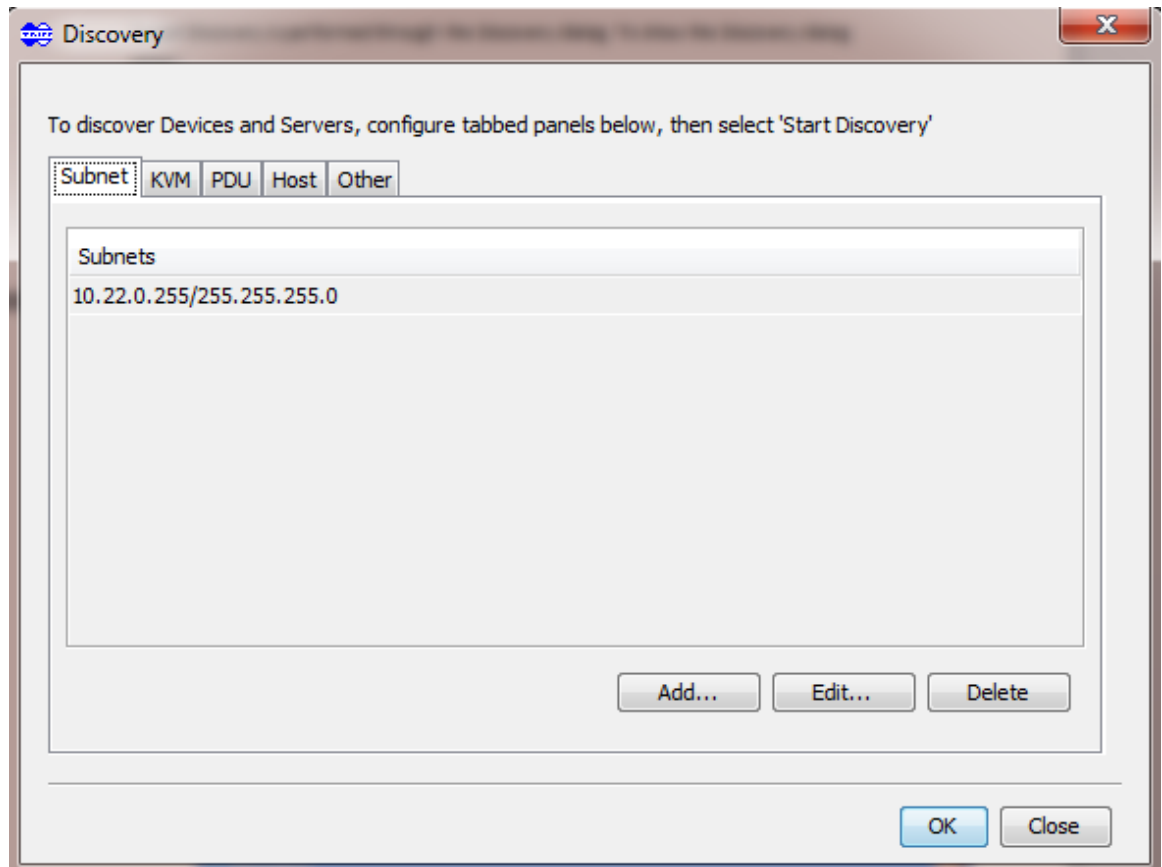
- Select the Discovery toolbar button
- Select Actions->Discovery main menu item

Two activities are performed by the user in this dialog:

- Configuring parameters for discovery

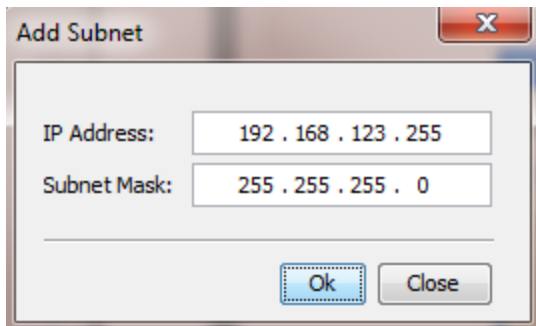
- Running the discovery itself

Below is an image of the loaded dialog:



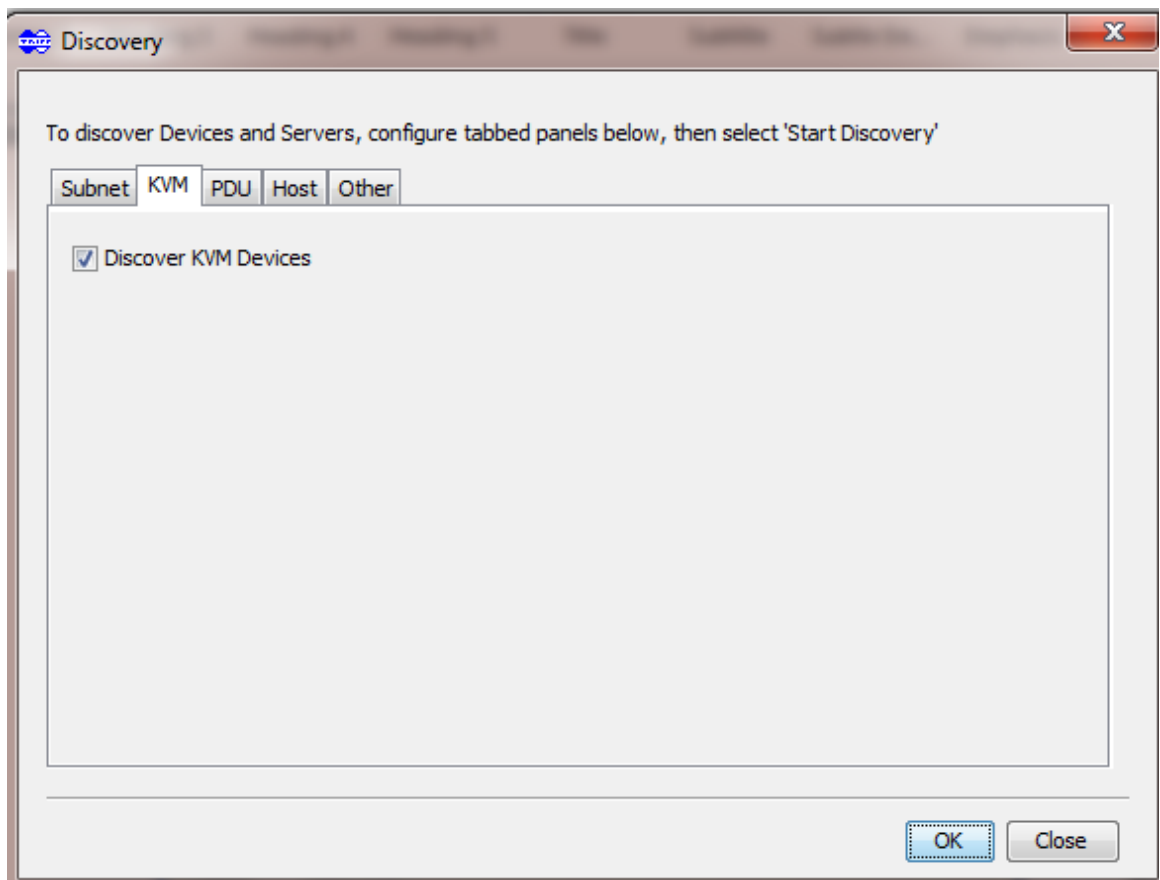
Discovery configuration parameters include:

- Subnets Tab:  
Provides definitions of subnets that will be searched for KVM & PDU devices and/or Hosts.
  - Subnets. Configuration of one or more subnets is done here. For a new Document, the subnets table is initialized with the local subnet. Discovery will attempt to discover KVM and PDU Devices within these subnets. Below is an image of the dialog used for adding a subnet. In the example, subnet 192.68.123.255 with with a mask of 255.255.255.0 shown:



- KVM Tab:  
Defines intent for discovering KVM devices.

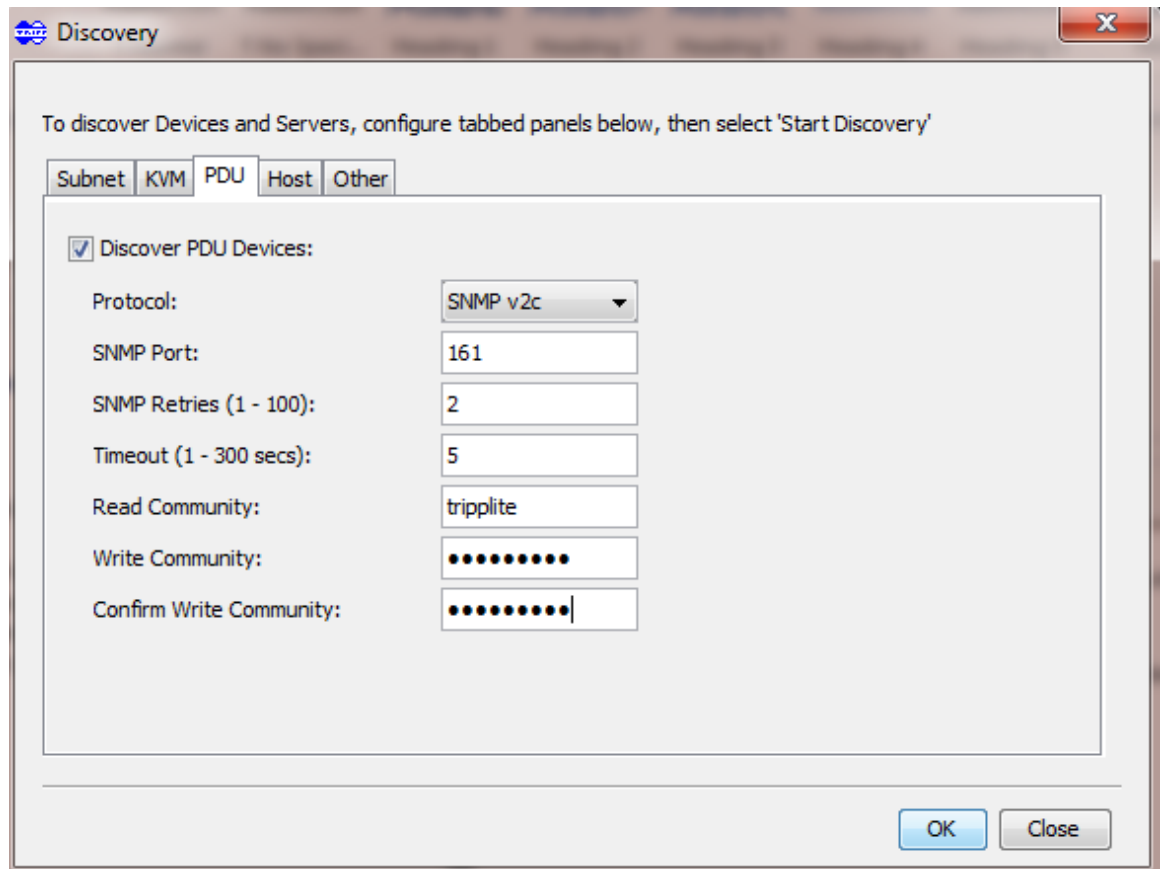
Example shown below:



Simply check / uncheck intent to subsequently discover KVM devices.

- PDU Tab:  
Defines intent and details for discovering PDU devices.

Example shown below:



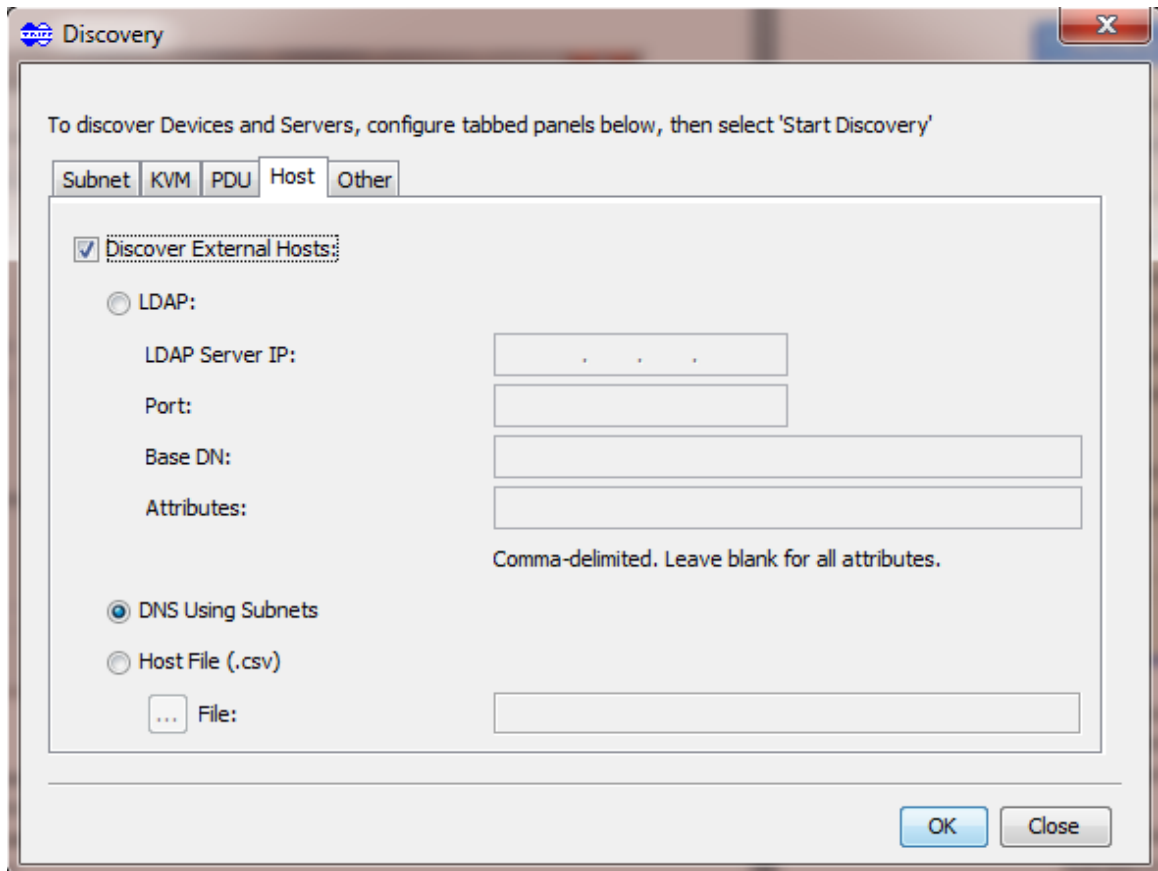
Details include:

- Check box for intent to discover PDU devices
- SNMP protocol to communicate with SNMP device (SNMP v1 or SNMP v2c)
- SNMP communications port
- SNMP retry count
- SNMP timeout period
- SNMP read and write communities

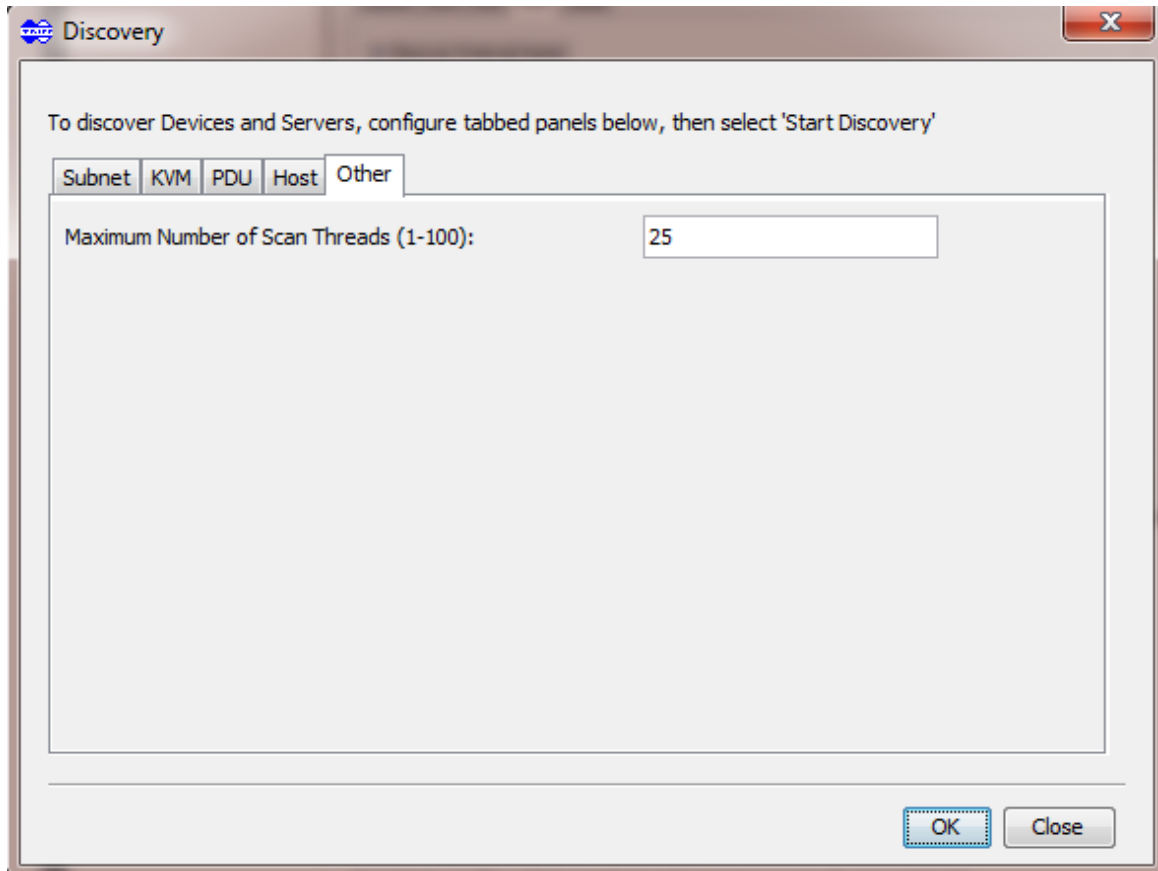
- Host Tab:

Configures intent and parameters for discovering/loading external hosts. When discovery is complete, these hosts can be dragged onto discovered targets to assist in name recognition of endpoints of targets.

Example shown below:



- LDAP choice and fields:  
Parameters for an LDAP server and LDAP query whose results will be treated as hosts. See the External Hosts section for more details in using LDAP for external hosts.
- DNS choice:  
Subnets in subnets tab will be inspected for DNS entries. Any DNS host names discovered will be used.
- Host File (csv) choice and file indication  
Supplied .csv file will be loaded and treated as a set of external hosts.
- Other Tab:  
Configures number of maximum number of threads that can run concurrently in discovery.  
Example shown below:



Once configuration has been set up, to start a discovery session, select the “Start Discovery” button. See the image in the Quick Start section for an example of a running Discovery session.

After a discovery session has completed, a table of discovered KVM and PDU Targets and external hosts is shown. In the table, the user can:

- Delete discovered KVM and PDU Targets that are of no interest.
- Drag external host names of interest onto relevant Targets
- Manually edit names of Targets

Finally, selecting OK will place the discovered Targets together with discovered Devices into NetCommander-AXS Window for further use.

## User Authentication

Prior to allowing access and usage of a Document, the NetCommander-AXS will authenticate the user. Authentication occurs when accessing the Document either with Access Mode or Admin Mode.



Part of a Document's definition is its authentication mode. There are 4 such modes:

- No Authentication. No authentication is performed and any user can access the Document, in Access Mode or Admin Mode.
- Document-Defined User Authentication. An encrypted list of user name + password pairs are defined within the Document. The user's user name and password is authenticated with this list.
- LDAP Authentication. The user provides a user name and password, which is authenticated with one or more LDAP servers. Additionally, trying to display a Target may require additional authentication.
- RADIUS Authentication. The user provides a user name and password, which is authenticated with one or more LDAP servers.

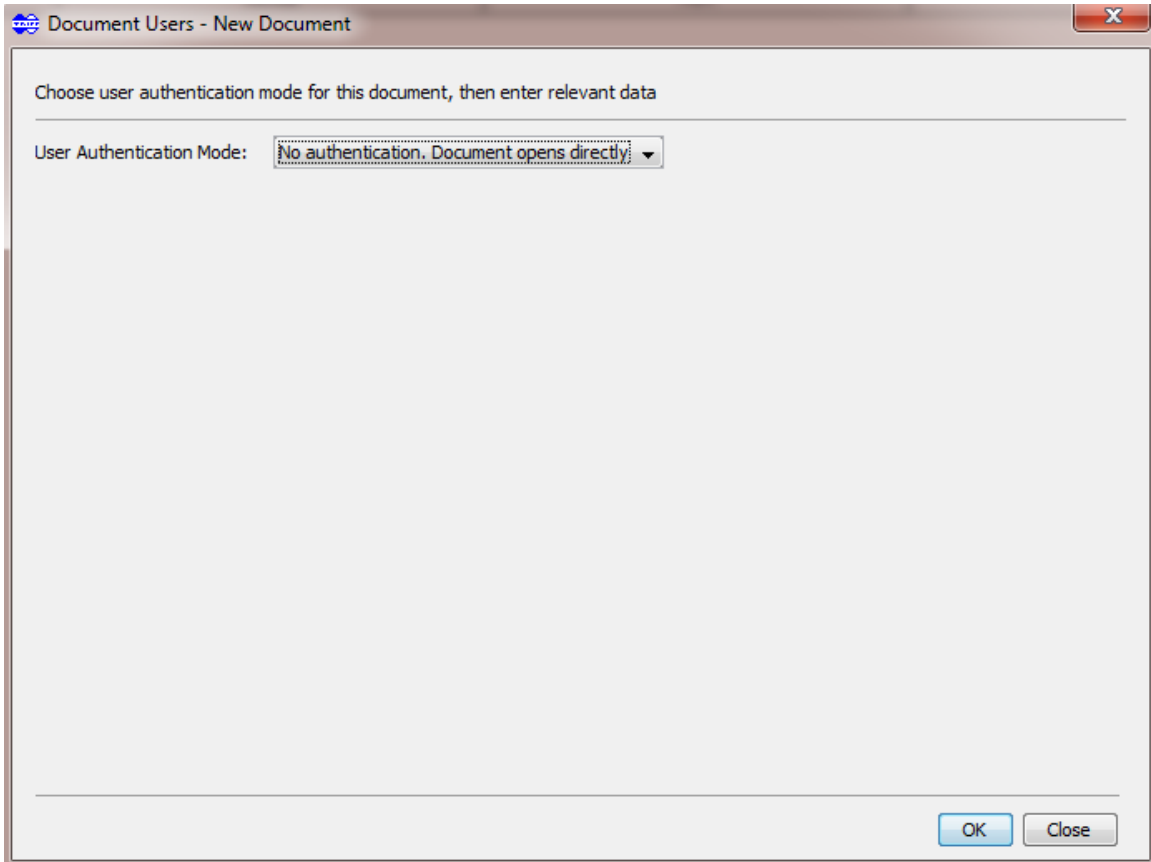
Defining user authentication mode for a Document is done through Admin Mode. The user must define an authentication mode when saving a Document for the first time.

Additionally, the Users dialog, which manages authentication definitions, can be accessed from the Options->Users main menu item or the Users toolbar button. This allows for editing the Document's User Authentication mode and content in ongoing fashion as desired.

Details of the different definitions are presented in the next sections.

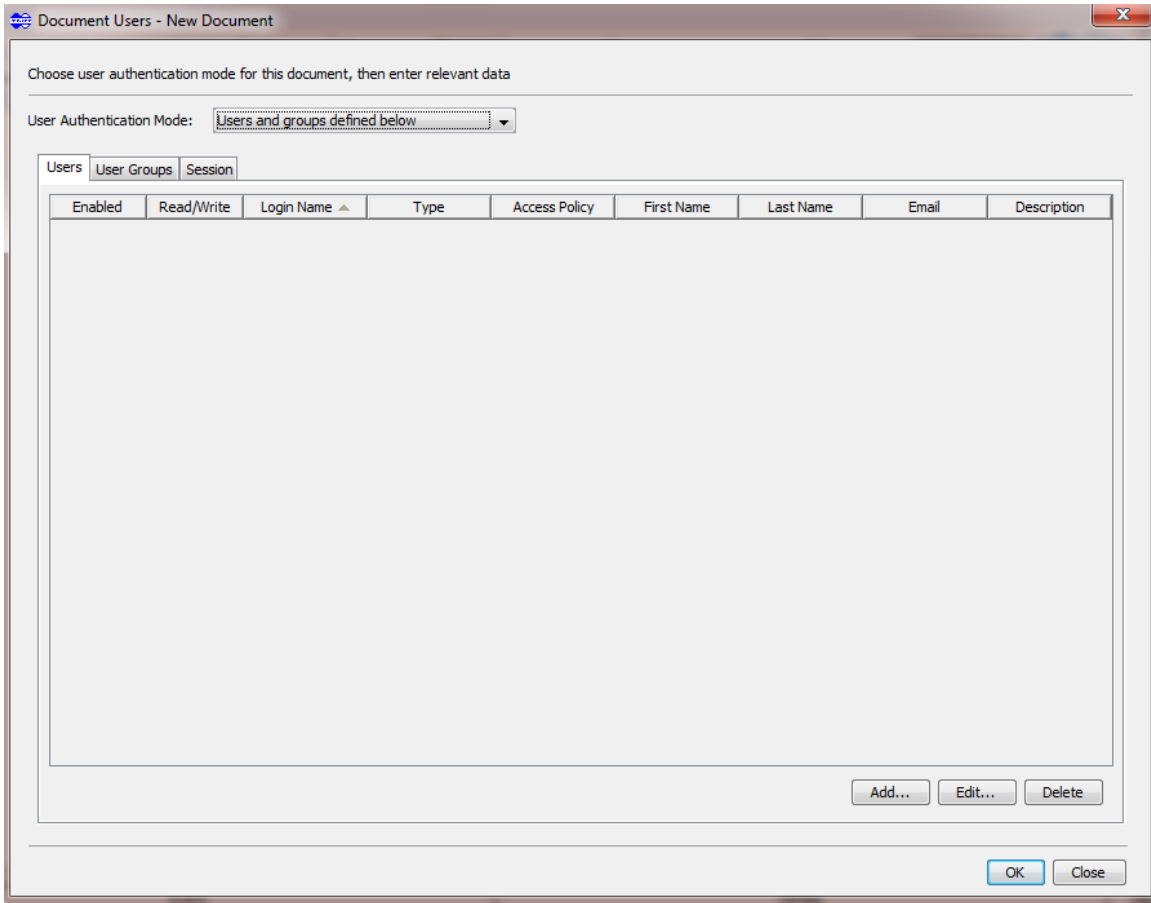
## **No Authentication Mode**

To define a situation where free access is given to a Document, use the No Authentication Mode. Simply select the 'No authentication. Document opens directly' combo box item. Image of this choice is shown below:



## Document-Defined User Authentication

To define Document-defined user authentication mode, select the 'Users and groups defined below' combo box item. The users, users groups, and session tabbed pane is shown. See below:



In the Users tab, you can add, edit, and delete users as needed. Below is the dialog shown for adding /editing a user:

The image shows a 'New User' dialog box with the following fields and options:

- Login Name: [Text Input]
- Password: [Text Input]
- Confirm Password: [Text Input]
- User Type: [Dropdown Menu, currently showing 'User']
- First Name: [Text Input]
- Last Name: [Text Input]
- Email: [Text Input]
- Description: [Text Input]
- Read/Write
- Enabled
- Access Policy: [Dropdown Menu, currently showing 'All Targets']

Buttons: OK, Cancel

Fields required to be filled out are:

- Login name. User name in login dialog
- Password. Password in login dialog
- User type. User or Administrator. ('User' type implies access for Access Mode only.)
- Read/write. Relevant for limiting Administrator users to be read/write or read-only, as well as User users to be read/write or read-only. For User users, this is relevant only for PDU targets, where a read/write user could manipulate an outlet's status, whereas a read-only user cannot.
- Enabled. If not selected, user will not be allowed to login.
- Access Policy. Defines range of targets/devices user can access. See discussion below.

## Access Policy

Access policy indicates which devices and/or targets the referenced user has access to. Choices are:

- All Targets. If selected, the user has access to all defined targets in the Document. For Admin type users, this must be selected.
- Selected Devices. If selected, user has access to any targets defined within the selected device(s). See example below.
- Selected Targets. If selected, user has access to any target(s) selected. See example below.

- Selected User Group. If selected, user has access to targets defined within the user group. See discussion on user groups.

## Selected Devices Example

User 'user\_a' is limited to viewing and accessing the targets within the selected devices indicated:

The screenshot shows a 'New User' dialog box with the following fields and options:

- Login Name: user\_a
- Password: [masked]
- Confirm Password: [masked]
- User Type: User
- First Name: [empty]
- Last Name: [empty]
- Email: [empty]
- Description: [empty]
- Read/Write:
- Enabled:
- Access Policy: Selected Devices:

	Device Name ▲	Group	IP	Type
<input type="checkbox"/>	192.168.123.73	Our KVMs	192.168.123.73	Tripp Lite 2x32 KVM
<input checked="" type="checkbox"/>	192.168.123.82	Our KVMs	192.168.123.82	Tripp Lite 1x16 KVM
<input checked="" type="checkbox"/>	192.168.123.88	Our KVMs	192.168.123.88	Tripp Lite 2x16 KVM
<input type="checkbox"/>	192.168.123.252	Our PDUs	192.168.123.252	Tripp Lite 30 Port ...

Buttons: OK, Cancel

## Selected Targets Example

User 'user\_b' is limited to viewing and accessing the targets indicated:

**New User** [Close]

Login Name:

Password:

Confirm Password:

User Type:

First Name:

Last Name:

Email:

Description:

Read/Write

Enabled

Access Policy:

	Target Name ▲	Group	Device	Port
<input type="checkbox"/>	zenith Primero	Corporate Access	192.168.123.88	12
<input checked="" type="checkbox"/>	IWC Schaffhausen	Corporate Access	192.168.123.88	13
<input type="checkbox"/>	Rolex Submariner	Corporate Access	192.168.123.88	14
<input checked="" type="checkbox"/>	Audemars Piguet R...	Corporate Access	192.168.123.88	15
<input checked="" type="checkbox"/>	Ulysse Nardin	Corporate Access	192.168.123.88	16
<input type="checkbox"/>	192.168.123.252 ...	Power	192.168.123.252	1
<input type="checkbox"/>	192.168.123.252 ...	Power	192.168.123.252	2
<input checked="" type="checkbox"/>	192.168.123.252 ...	Power	192.168.123.252	3
<input checked="" type="checkbox"/>	192.168.123.252 ...	Power	192.168.123.252	4
<input checked="" type="checkbox"/>	192.168.123.252 ...	Power	192.168.123.252	5
<input type="checkbox"/>	192.168.123.252 ...	Power	192.168.123.252	6

OK Cancel

## User Groups

User groups are sets of users who are given a common access policy. User groups makes it easy to define many users with a common user policy. Below are 2 examples.

## Group with Selected Devices Example

**Edit User Group**

Name:

Description:

Selected Users in Group:

	Enabled	User Name ▲	Type	Access Policy	First Name	Last Name	Email	Description
<input checked="" type="checkbox"/>	Yes	user1	User	User Group: group_a				
<input checked="" type="checkbox"/>	Yes	user2	User	User Group: group_a				
<input checked="" type="checkbox"/>	Yes	user3	User	User Group: group_a				
<input checked="" type="checkbox"/>	Yes	user4	User	User Group: group_a				
<input checked="" type="checkbox"/>	Yes	user5	User	User Group: group_a				
<input type="checkbox"/>	Yes	user6	User	All Targets				
<input type="checkbox"/>	Yes	user7	User	All Targets				
<input type="checkbox"/>	Yes	user8	User	All Targets				
<input type="checkbox"/>	Yes	admin	Administrator	All Targets				

Access Policy for Selected Users:

	Device Name ▲	Group	IP	Type
<input checked="" type="checkbox"/>	192.168.123.73	Our KVMs	192.168.123.73	Tripp Lite 2x32 KVM
<input type="checkbox"/>	192.168.123.82	Our KVMs	192.168.123.82	Tripp Lite 1x16 KVM
<input type="checkbox"/>	192.168.123.88	Our KVMs	192.168.123.88	Tripp Lite 2x16 KVM
<input checked="" type="checkbox"/>	192.168.123.252	Our PDUs	192.168.123.252	Tripp Lite 30 Port PDU (PDU3VSR2)

# Group with Selected Targets Example

**Edit User Group**

Name:

Description:

Selected Users in Group:

	Enabled	User Name ▲	Type	Access Policy	First Name	Last Name	Email	Description
<input type="checkbox"/>	Yes	user1	User	User Group: group_a				
<input type="checkbox"/>	Yes	user2	User	User Group: group_a				
<input type="checkbox"/>	Yes	user3	User	User Group: group_a				
<input type="checkbox"/>	Yes	user4	User	User Group: group_a				
<input type="checkbox"/>	Yes	user5	User	User Group: group_a				
<input checked="" type="checkbox"/>	Yes	user6	User	User Group: group_b				
<input checked="" type="checkbox"/>	Yes	user7	User	User Group: group_b				
<input checked="" type="checkbox"/>	Yes	user8	User	User Group: group_b				
<input type="checkbox"/>	Yes	admin	Administrator	All Targets				

Access Policy for Selected Users:

	Target Name	Group	Device	Port
<input checked="" type="checkbox"/>	SeaMaster Planet Ocean	Corporate Access	192.168.123.88	4
<input checked="" type="checkbox"/>	Superocean	Corporate Access	192.168.123.88	8
<input checked="" type="checkbox"/>	Navitimer	Corporate Access	192.168.123.88	10
<input checked="" type="checkbox"/>	Ulysse Nardin	Corporate Access	192.168.123.88	16
<input checked="" type="checkbox"/>	192.168.123.252 outlet 8	Power	192.168.123.252	8
<input checked="" type="checkbox"/>	192.168.123.252 outlet 11	Power	192.168.123.252	11
<input checked="" type="checkbox"/>	192.168.123.252 outlet 14	Power	192.168.123.252	14
<input checked="" type="checkbox"/>	192.168.123.252 outlet 17	Power	192.168.123.252	17
<input checked="" type="checkbox"/>	192.168.123.252 outlet 20	Power	192.168.123.252	20
<input type="checkbox"/>	Server 01	Maintenance Access	192.168.123.73	1
<input type="checkbox"/>	Server 02	Maintenance Access	192.168.123.73	2
<input type="checkbox"/>	Server 03	Maintenance Access	192.168.123.73	3
<input type="checkbox"/>	Server 04	Maintenance Access	192.168.123.73	4

OK Cancel



## Users Groups Tab for Group Examples Above

Document Users - demo\_sample

Choose user authentication mode for this document, then enter relevant data

User Authentication Mode:

Users | **User Groups** | Session

User Group Name ▲	Access Policy	Description
group_a	Selected Devices	
group_b	Selected Targets	

Add... Edit... Delete

OK Close

## Users Tab for Group Examples Above

Document Users - demo\_sample

Choose user authentication mode for this document, then enter relevant data

User Authentication Mode:

Users | **User Groups** | Session

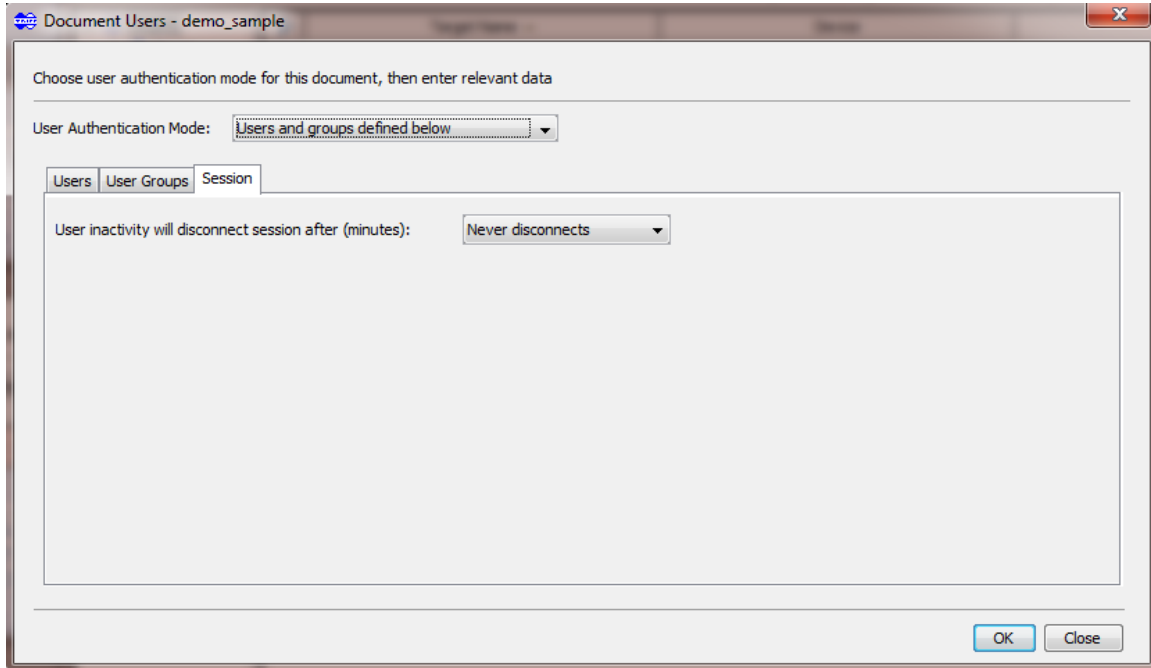
Enabled	Read/Write	Login Name ▲	Type	Access Policy	First Name	Last Name	Email	Description
Yes	Yes	user1	User	User Group: group_a				
Yes	Yes	user2	User	User Group: group_a				
Yes	Yes	user3	User	User Group: group_a				
Yes	Yes	user4	User	User Group: group_a				
Yes	Yes	user5	User	User Group: group_a				
Yes	Yes	user6	User	User Group: group_b				
Yes	Yes	user7	User	User Group: group_b				
Yes	Yes	user8	User	User Group: group_b				
Yes	Yes	admin	Administrator	All Targets				

Add... Edit... Delete

OK Close

## Session

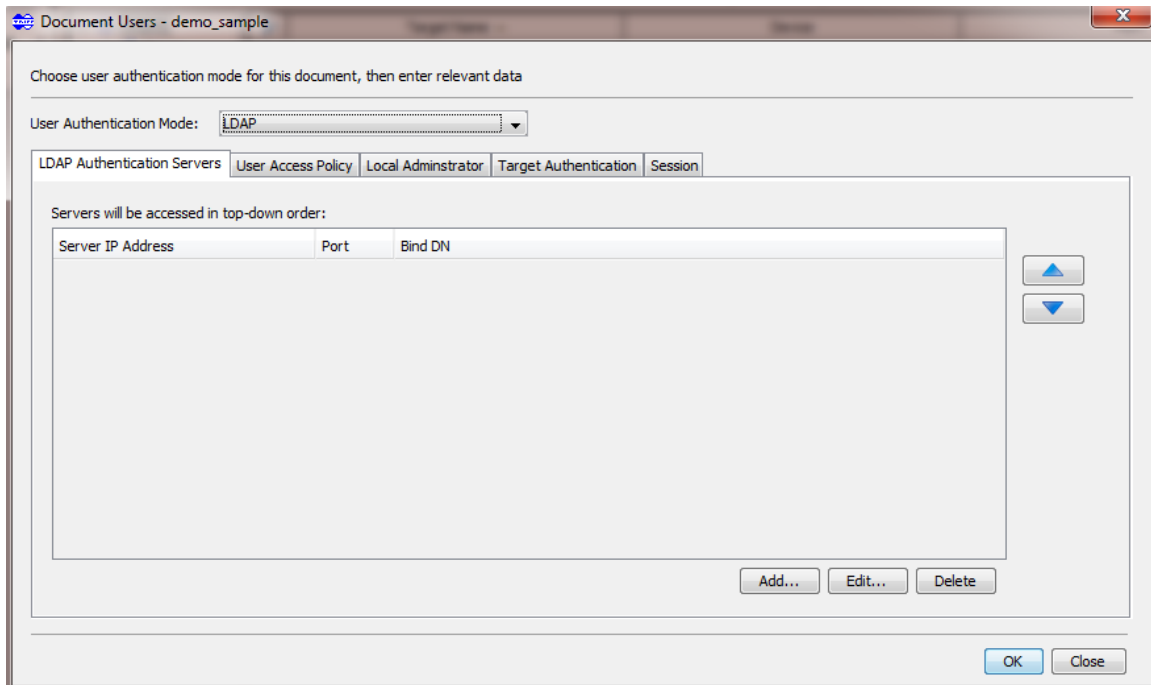
The last tab in this mode is the Session tab. It allows the user to define session disconnection after a period of user inactivity. Disconnection period choices are 'Never disconnects', 1, 5, 10, 15, 30, and 60 minutes. Tab view:



## LDAP Authentication

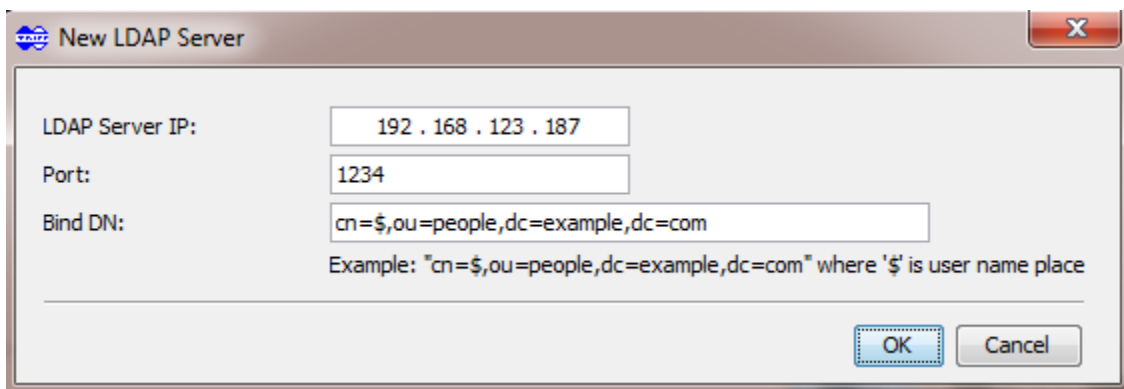
To define LDAP authentication mode, select the 'LDAP authentication' combo box item. The LDAP tabbed pane is shown.

To define LDAP authentication mode, select the 'LDAP' combo box item. LDAP Authentication Servers, User Access Policy, Local Administrator, Target Authentication, and Session tabbed pane is shown. See below:



## LDAP Servers

In the LDAP Authentication Servers tab, you can add, edit, and delete LDAP servers as needed. When authenticating a user, authentication will be performed top-down in the list if there are multiple servers defined. Below is the dialog shown for adding /editing an LDAP server:



The required items to define this mode include:

- LDAP server IP. The IP address of the LDAP server to be used for authentication
- Port. Port number of the LDAP server to be used for authentication
- Bind DN. The LDAP Bind DN to be used in authenticating a user. The bind DN must include a '\$' character which represents a place-holder for the user name.
  - An example of a bind DN:  
cn=,ou=people,dc=example,dc=com

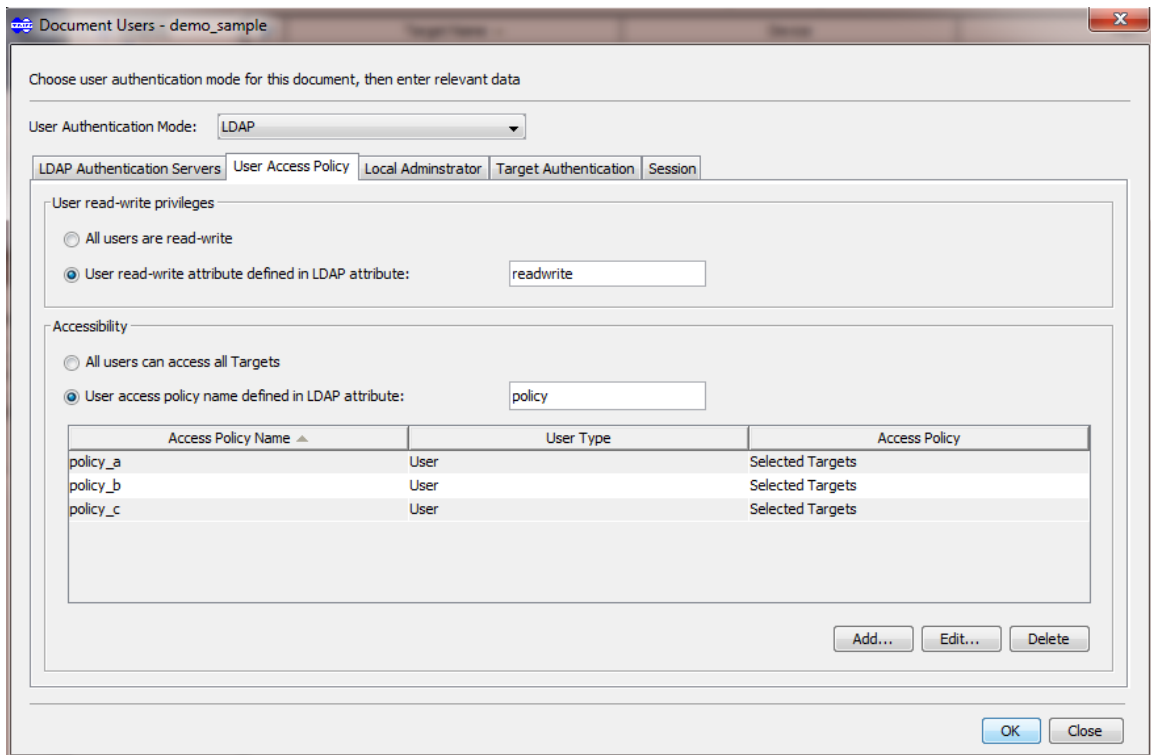
If a user tries to login as user: Yaron, an attempt to authenticate with bind DN of cn=Yaron,ou=people,dc=example,dc=com will be performed.

- Declaration of users read/write attribute. 2 choices are:
  - All users are read-write
  - Value of LDAP attribute to be inspected if user is read-write. A value of 'yes' implies read-write, 'no' implies read-only.
- Admin user name and password. This user name and password are intended as a back-door access to the document if the LDAP server becomes unusable.

## User Access Policy

User attributes are defined in the User Access Policy tab. See image below.

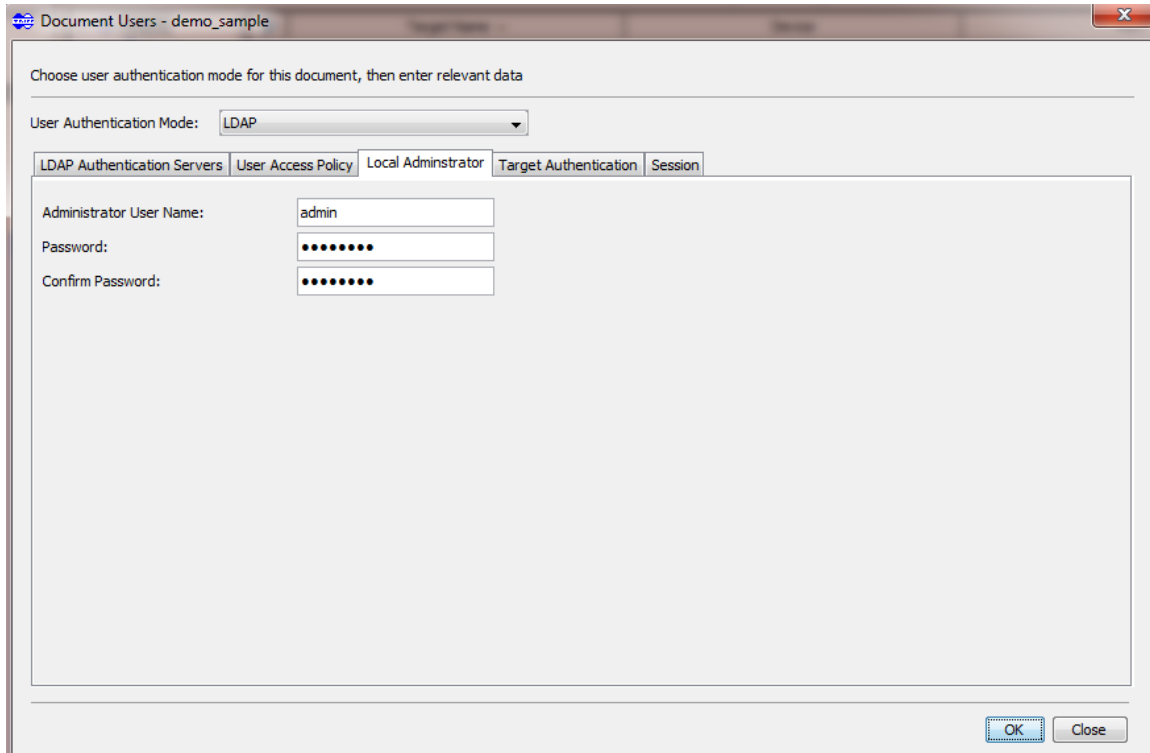
- User read-write attribute
  - Select either 'All users are read-write' or
  - 'User read-write attribute defined in LDAP attribute:' to allow read-write on a per user basis. In the example below, user attribute 'readwrite' defines user having read-write privileges or not.
  -
- Accessibility attribute
  - Select either 'All users can access all targets' or
  - 'User access policy name defined in LDAP attribute:' to define LDAP attribute containing the name of relevant user policy on a per-user basis. In the example below, user attribute 'policy' defines the access policy name relevant for each user.



## Local Administrator

An administrator user will be defined as a 'local administrator'. That is, access will be provided to this user regardless of LDAP's status. This allows access to the Document in the event that LDAP services are unavailable.

Below is an example of this panel.



## Target Authentication

Choices are:

- No authentication. A user that has already been LDAP authenticated at the Document level has free access to any Targets.
- Authenticate with LDAP filter. In this case the following information must be defined:
  - LDAP Server IP. The IP address of the LDAP server to be used for target authentication. (Note that this can be different from the Documentation-level authentication LDAP server.)
  - Port. Port number of the LDAP server to be used for authentication
  - Authorization Subtree DN. The DN used for authenticating the Target access rights
  - Device Name Attribute. Attribute for representing the KVM device name for which authentication will be allowed.
  - Users Access Attribute. The attribute representing instances of user names and Target port lists for which these users have authentication privileges. Within the LDAP definition itself, the NetCommander-AXS requires this field to be valued in the following syntax: <user\_name>,<portnum\_1>,<portnum\_2>,...<portnum\_n> where:
    - <user\_name> is the user name
    - And <portnum\_1>, <portnum\_2>,...<portnum\_n> is a comma-delimited list of port numbers such that Targets with those port numbers will be authenticated. (See example).

An indication of what user name to use when authenticating the Target.

Choices:

- Prompt for user name and password on target access. The user will be shown a login dialog for the target, and the resulting user name and password will be used for target authentication.
- Authenticate with logged in user credentials on target access. The already-authenticated user name and password from the Document-level authentication will be used.

Below is an example of the Target Authentication tab

The screenshot shows a dialog box titled "Document Users - New Document" with a close button in the top right corner. The main instruction is "Choose user authentication mode for this document, then enter relevant data". A dropdown menu for "User Authentication Mode" is set to "LDAP". Below this are five tabs: "LDAP Authentication Servers", "User Access Policy", "Local Administrator", "Target Authentication" (which is selected), and "Session".

Under the "Target Authentication" tab, there are two radio button options:

- None. Authenticated document users have access to all targets
- Authenticate target access with LDAP filter:

Below the second option are several input fields:

- LDAP Server IP: 192 . 168 . 123 . 107
- Port: 1234
- Authorization Subtree DN: ou=accessdevices,dc=example,dc=com
- Device Name LDAP Attribute: cn
- Users Access LDAP Attribute: access

At the bottom of the dialog, there are two more radio button options:

- Prompt for user name and password on target access
- Authenticate with logged in user credentials on target access

At the bottom right of the dialog are "OK" and "Close" buttons.

## Session

See discussion in the Users and User Groups section

## Example of LDAP user definition

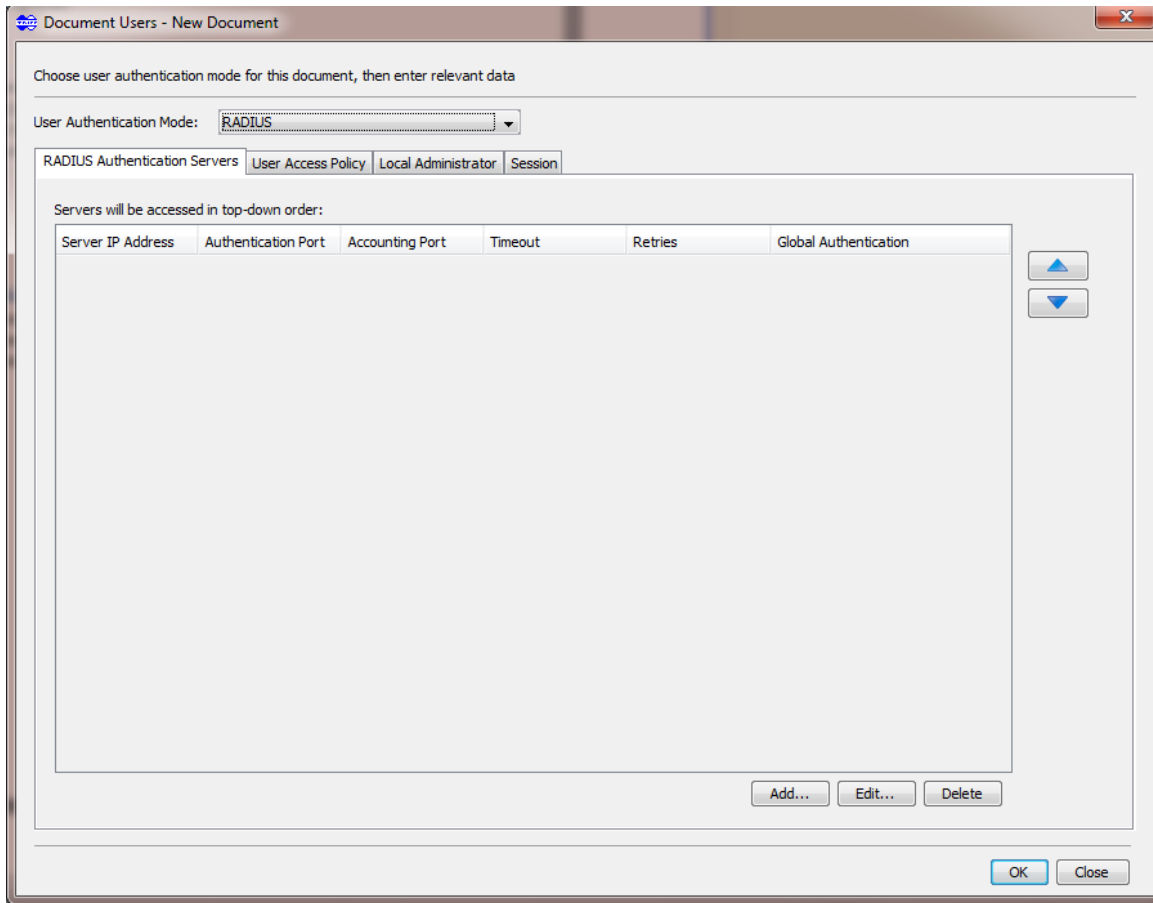
A typical example:

```
dn: cn=Yaron,ou=people,dc=example,dc=com
objectclass: inetOrgPerson
cn: Yaron
sn: yalfia
uid: yalfia
userpassword: yaron
carlicense: ZA-123-BB56
homephone: 515-555-1234
mail: yaron @yourcompany.com
description: mgr
readwrite: yes
policy:policy_a
```

## RADIUS Authentication

To define RADIUS authentication mode, select the 'RADIUS' combo box item. The RADIUS tabbed pane is shown. See below. The tabs presented are similar to their equivalents in LDAP. See LDAP section for details.





## Onboard Device Configuration

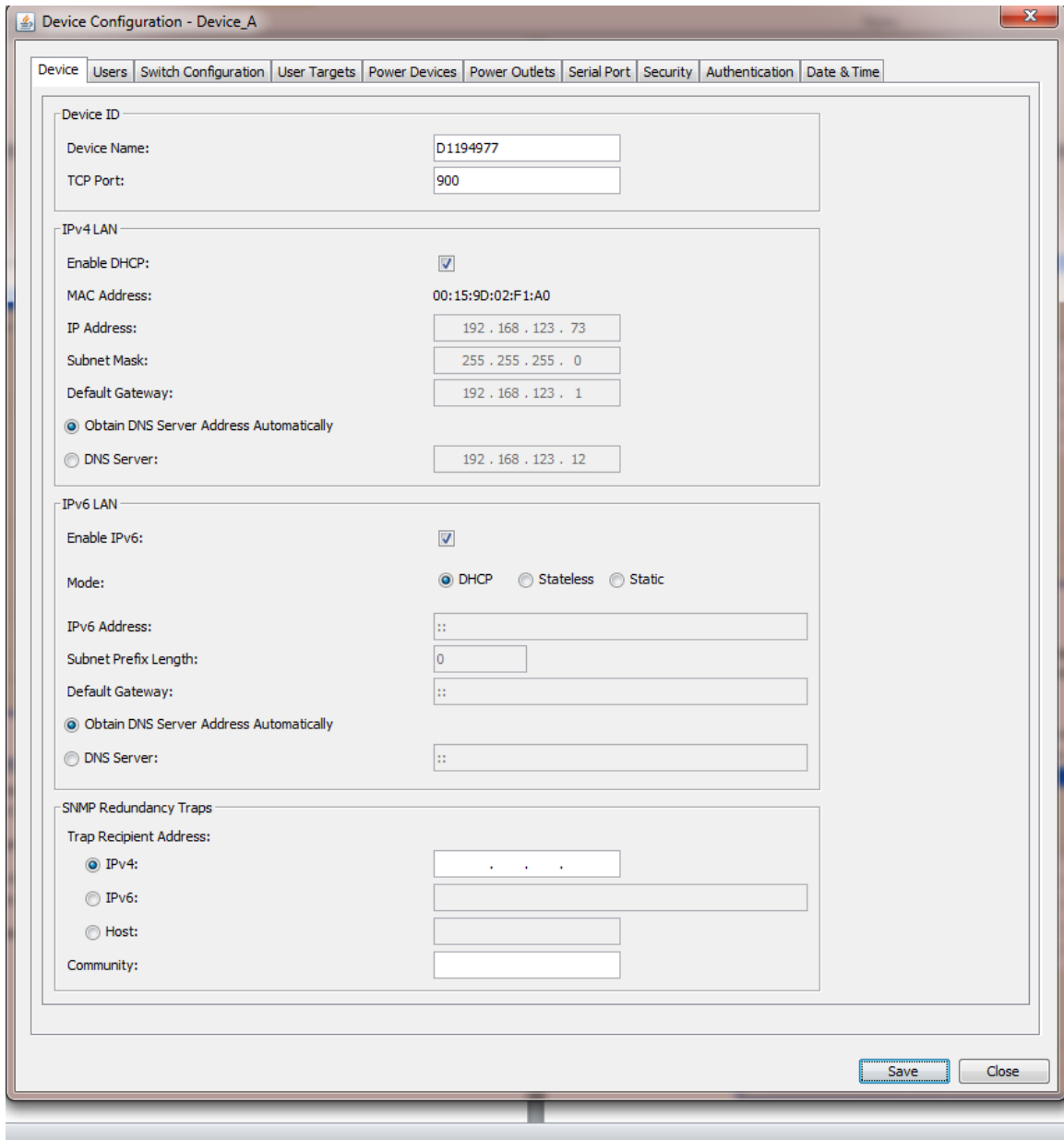
The NetCommander-AXS allows displaying and editing of the onboard configuration of a KVM Device.

This onboard device configuration shows and allows editing of configuration parameters directly on the device. This is the same configuration user interface available in Tripp Lite's NetCommander-IP Client product. A large set of parameters can be configured and saved to the device, such as IP address, device name, device date and time, etc.

To access onboard device configuration, select the KVM Device of interest in the KVM Devices table, and select the Device Configuration menu item in either:

- Popup menu
- Actions main menu

Below is an image of the Device Configuration dialog:



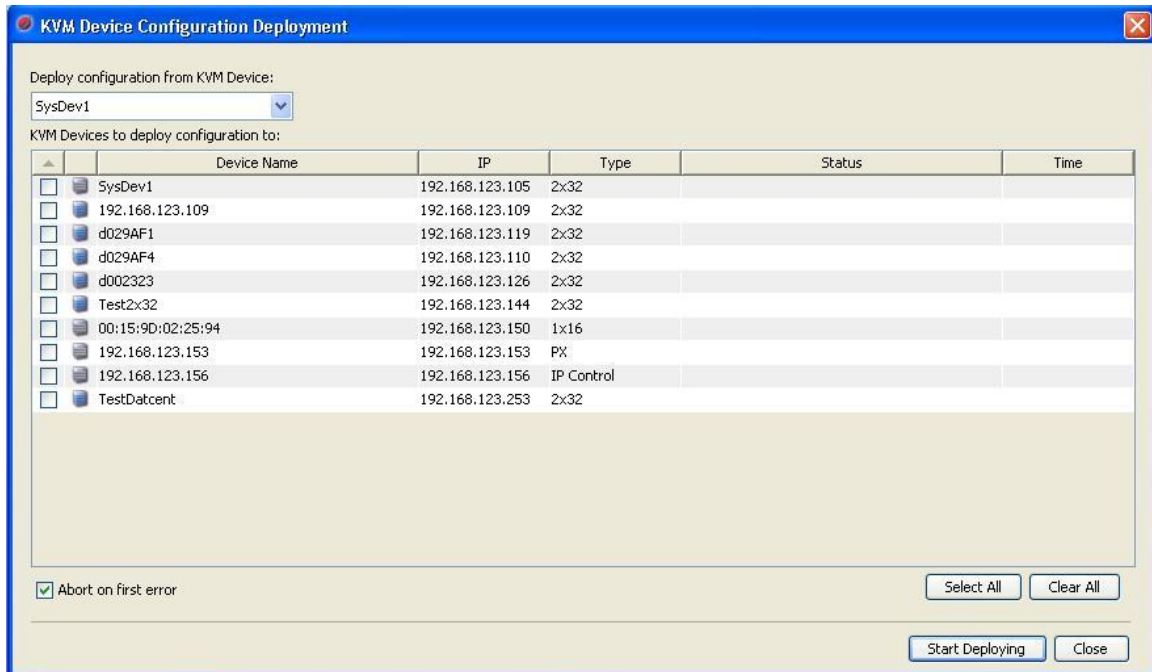
## Multi Device Onboard Configuration Deployment

The NetCommander-AXS provides for saving onboard configuration of a specific device to a selected list of other devices ("configuration deployment").

To access multi device onboard configuration deployment:

- Select the "Actions->KVM-> KVM Device Configuration Deployment..." or
- Select a Device, right-click, and pick the "KVM Device Configuration Deployment.."

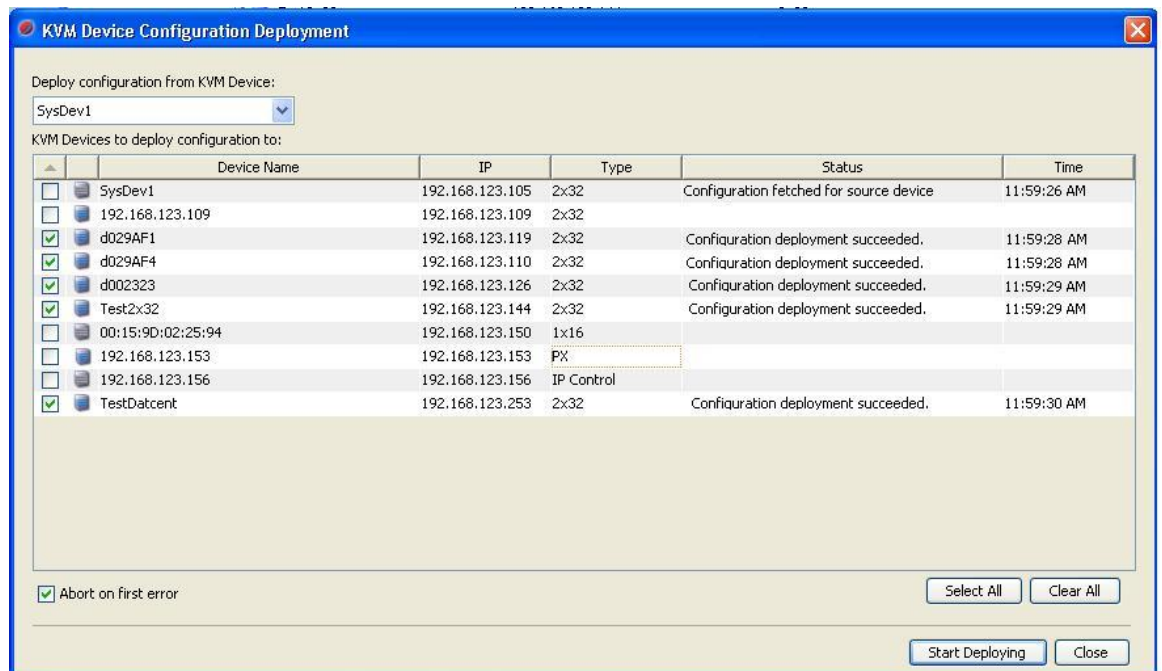
The following dialog is displayed:



To deploy configuration:

- 1) Select the source device whose configuration will be deployed in the combo box
- 2) Select the checkboxes of devices to save the configuration to.
- 3) Select 'Start Deploying'

Deployment then begins, and results are shown to user as they occur. Below is an example of configuration deployment after completion:

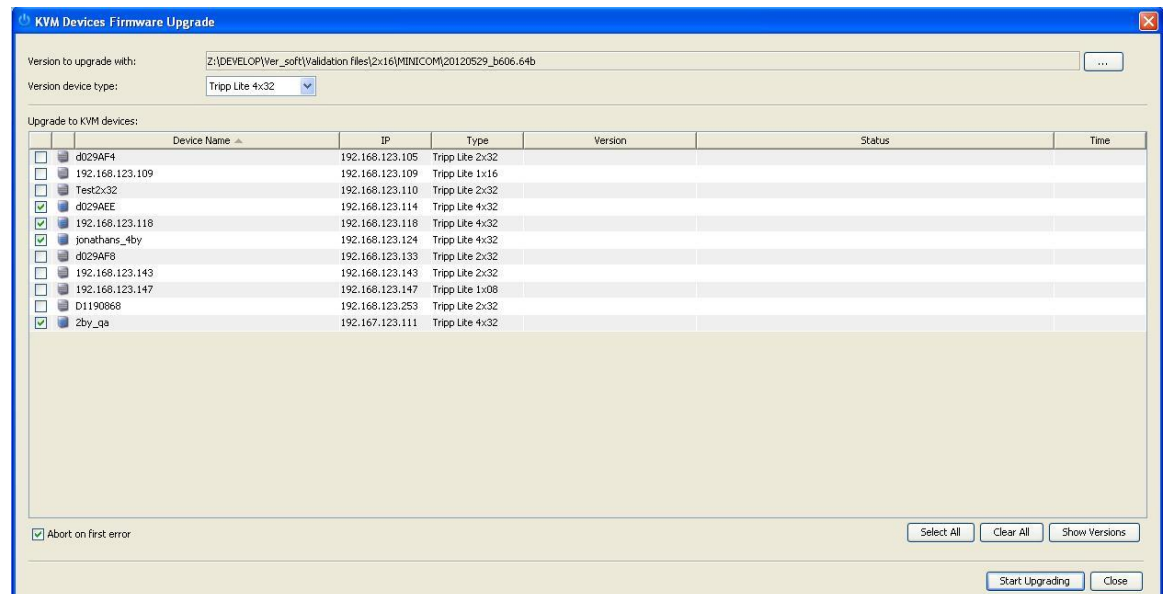


# Multiple Device Firmware Upgrade

In Admin mode, selecting the Actions->KVM->KVM Devices Firmware Upgrade... menu item will load the dialog, an example of which is shown below.

This dialog allows the user to upgrade an indicated firmware version to multiple selected devices. The user must:

- Reference the firmware file to upgrade with
- Select a device type of interest (4x32, 2x32, etc)
- Select check boxes of relevant devices for the type
- Indicate whether to abort on first error encountered
- Load current version numbers by selecting 'Show Versions' button
- Upgrade firmware by selecting 'Start Upgrading' button



## Reachability

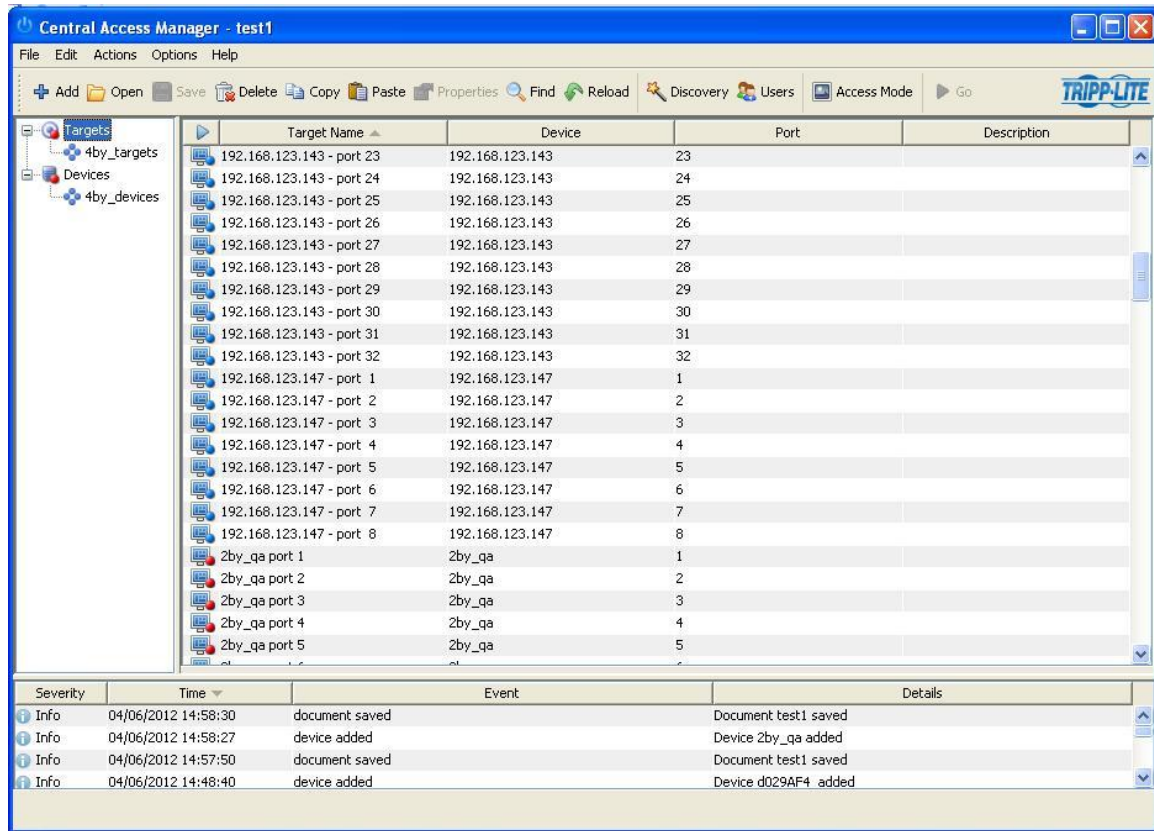
### Admin Mode

The Central Manager Window periodically updates the reachability states of any Groups, Devices, and Targets within it. A Device (and its associated Targets and Group) is considered reachable if there is communications with its IP address.

- If a Device, Target, or Group is reachable, no special adjustments to its associated icon is made.

- If a Device, Target, or Group is not reachable, a small red circle in the lower-right corner is shown in its associated icon

An example is shown below:

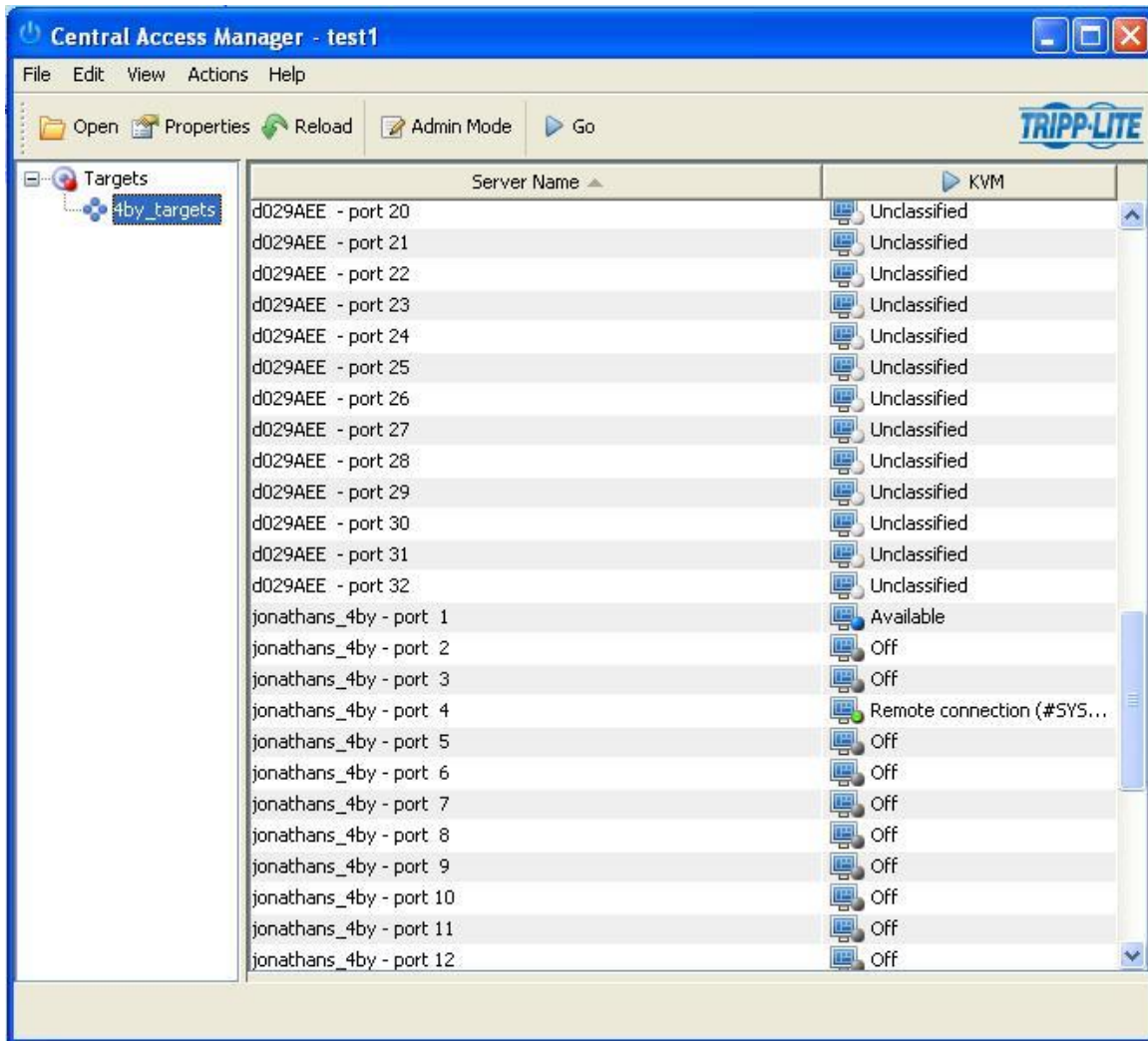


## Access Mode

In access mode, KVM targets' statuses include:

- Available (blue)
- Off (grey)
- Remote Connection (green)
- Unclassified (white)
- Busy (yellow)
- Not Reachable (red)

Below is an example:



For PDU targets, statuses include:

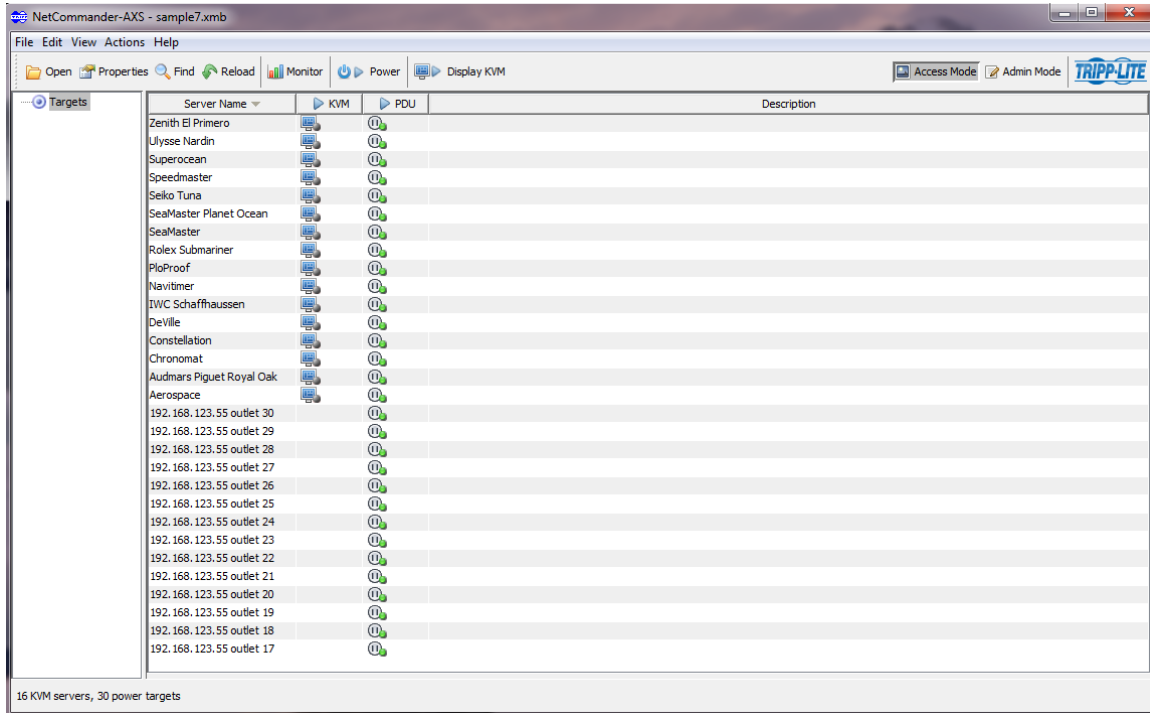
- Off (grey)
- Remote Connection (green)
- Unclassified (white)
- Not Reachable (red)

## KVM-to-Power

The software provides the ability to configure KVM and PDU targets within a given group such that they will have the same name, which will result in alignment of both targets on the same

row in the Targets table in Access Mode. This is often desired, since a PDU outlet is often associated with a given KVM target.

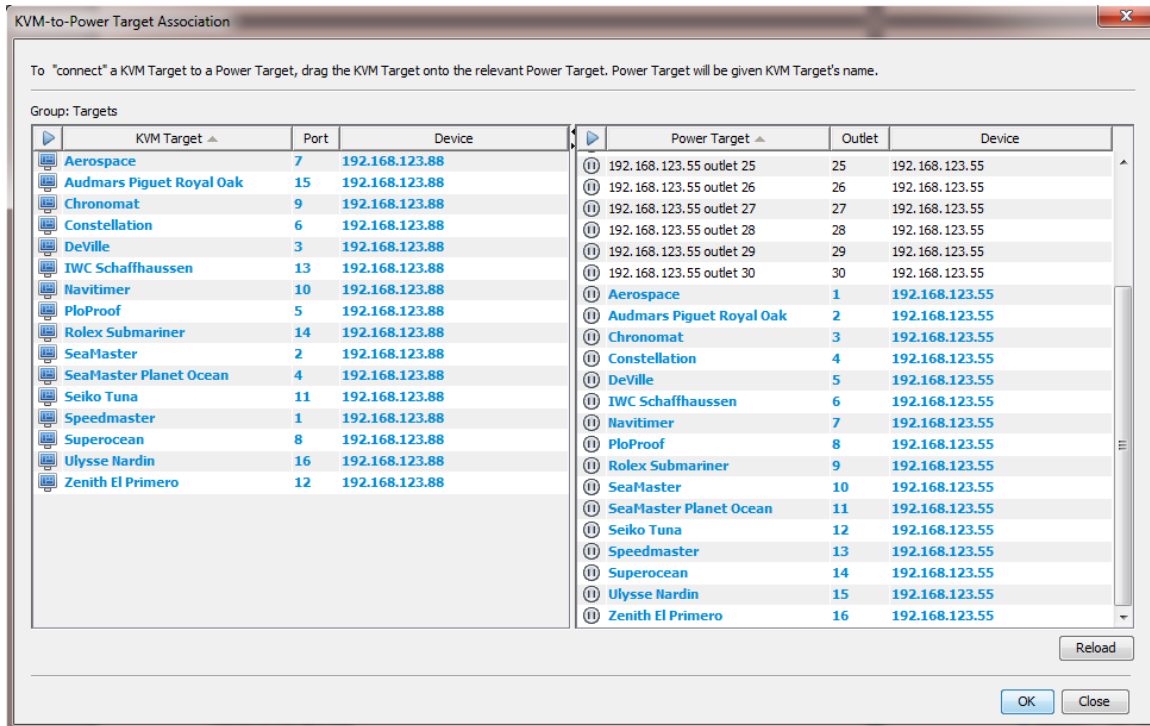
An example of this effect can be seen below.



To pair a KVM target with a PDU outlet within a TargetGroup, do the following:

- Open the Document of interest in Admin Mode.
- Select the Target group of interest, and set focus in the Targets table.
- Either:
  - Right-click and select KVM-to-Power
  - Select menu Actions->KVM->KVM-to-Power
- In the resulting KVM-to-Power dialog, drag-drop KVM target(s) of interest onto PDU outlet(s) of interest on the right-side.
- Select the OK button, and save the Document.

Below is an example of the KVM-to-Power dialog with the dragged results for the example shown above.



## KVM Targets Name Synchronization

When defining KVM devices within NetCommander-AXS, target names for a given KVM device will not necessarily reflect the Target names that are resident on the KVM device as seen through NetCommander IP Client. The NetCommander-AXS software provides a mechanism for the Admin user to “pull” target names from the KVM device onto their equivalent targets within NetCommander-AXS. Alternatively, the Admin user can “push” NetCommander-AXS target names onto their equivalent targets on the KVM device.

### Pull Target Names from Device

To “pull” target names from a given KVM device and overwrite the equivalent target within the NetCommander-AXS Document:

- Open the Document of interest in Admin mode
- Select the Devices tree node, and select the KVM device of interest in the Devices Table.
- Either:
  - Right-click and select Synchronize Targets->Pull Target Names from Device...”
  - Or select
  - Actions->KVM-> Synchronize Targets->Pull Target Names From Device...” menu item
- Accept the prompts.
- Confirm that target names are synchronized.

The relevant KVM target names in the NetCommander-AXS Document will be overwritten.



## Push Target Names to Device

To “push” target names for a KVM device within a specific Targets Group to the KVM device itself:

- Open the Document of interest in Admin mode
- Select the Devices tree node, and select the KVM device of interest in the Devices Table.
- Either:
  - Right-click and select Synchronize Targets->Push Target Names to Device...”
  - Or select
  - Actions->KVM-> Synchronize Targets-> Push Target Names to Device...” menu item
- Accept the prompts.
- Confirm that target names are synchronized.

## Additional Functionality

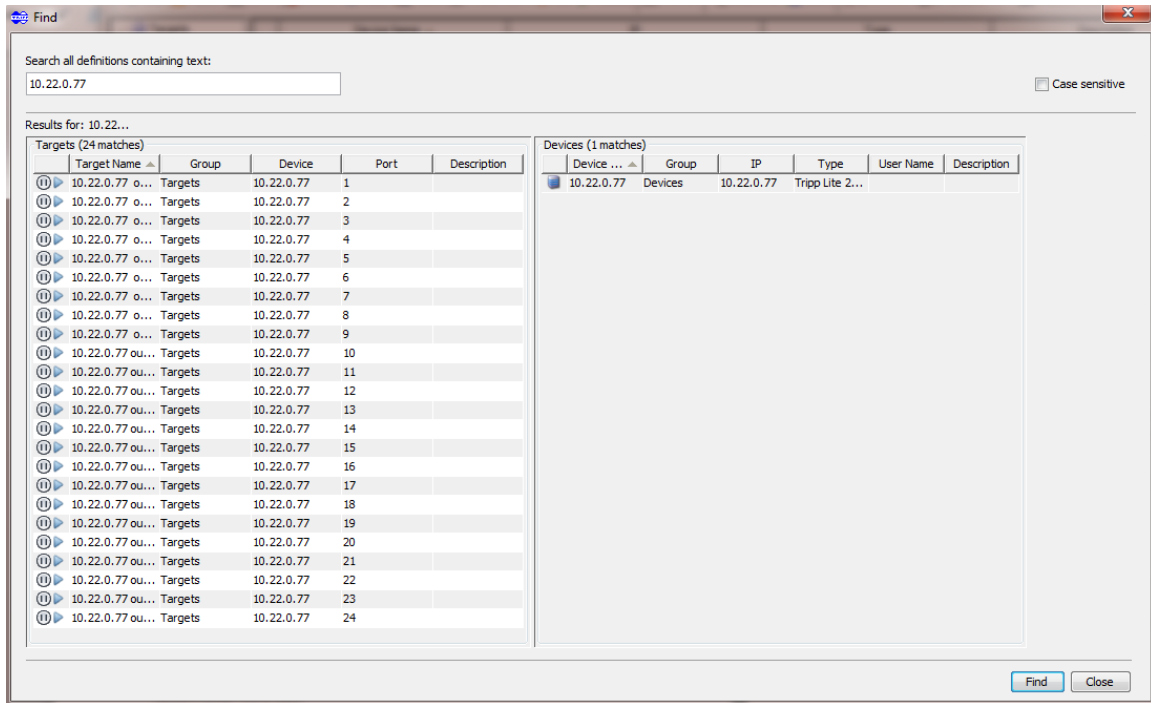
### Find

NetCommander-AXS provides a Find utility that will search on a supplied text fragment, attempting to match it into content for defined devices and targets.

The Find dialog can be opened by either:

- Selecting the Find toolbar button
- Selecting Edit->Find menu item

Below is an example of the results of a Find session:



Double-clicking on an entry in the results of a find session will select the equivalent entry in the relevant Devices or Targets table.

## Reload

Reload functionality is provided. Upon selecting reload, and changes to the current Document being edited is abandoned, and the last saved copy of the Document is reloaded into the NetCommander-AXS window.

To access Reload, select the Reload button in the main toolbar.

## Preferences

The NetCommander-AXS Admin user has the ability to affect certain look-and-feel as well as behavioral attributes of the software.

Attributes that can be configured include:

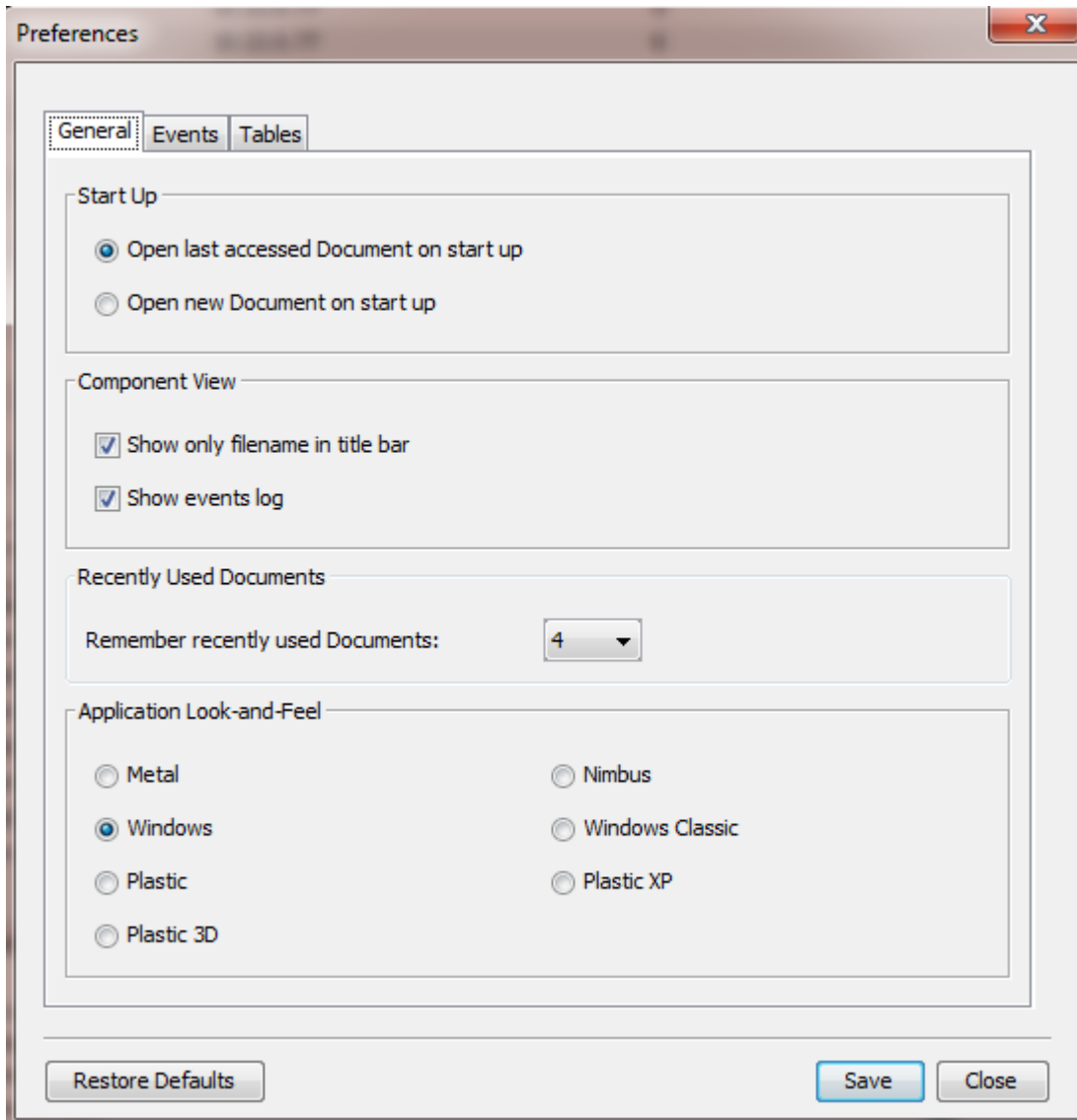
- When opening NetCommander-AXS, open with last accessed Document, or open a new Document
- Show filename only of the Document in the title bar, or the complete file path
- Configure maximum number of recently used Documents under the 'Open Recent' File submenu
- Configure Windows theme look-and-feel
- Configure maximum number of events that the events log can hold

- Enable/disable alternate shading of rows in tables
- Configure columns in Device and Target tables

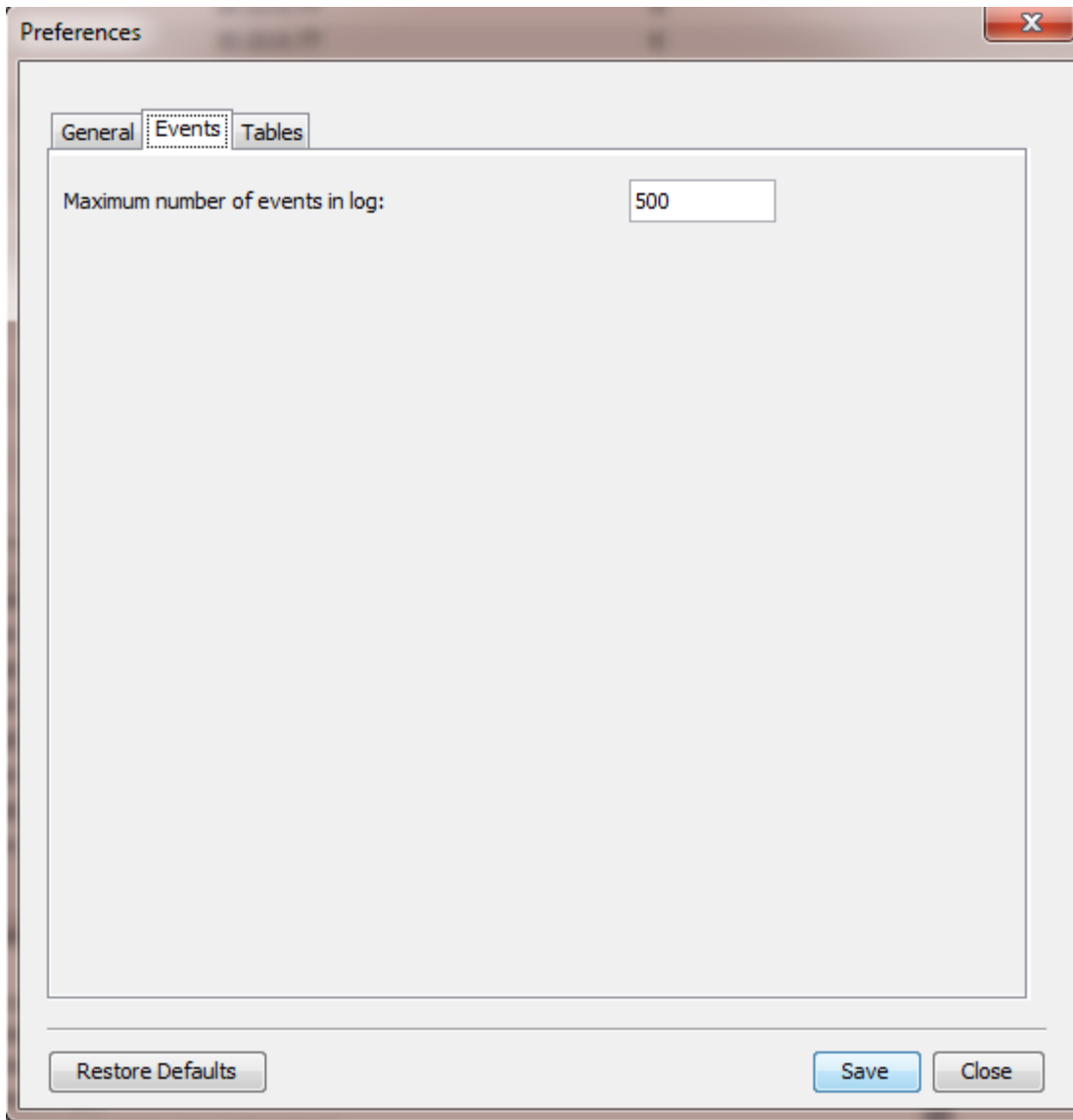
Saving Preferences persists across all Documents.

The Preferences dialog consists of 3 tabs: General, Events, and Tables

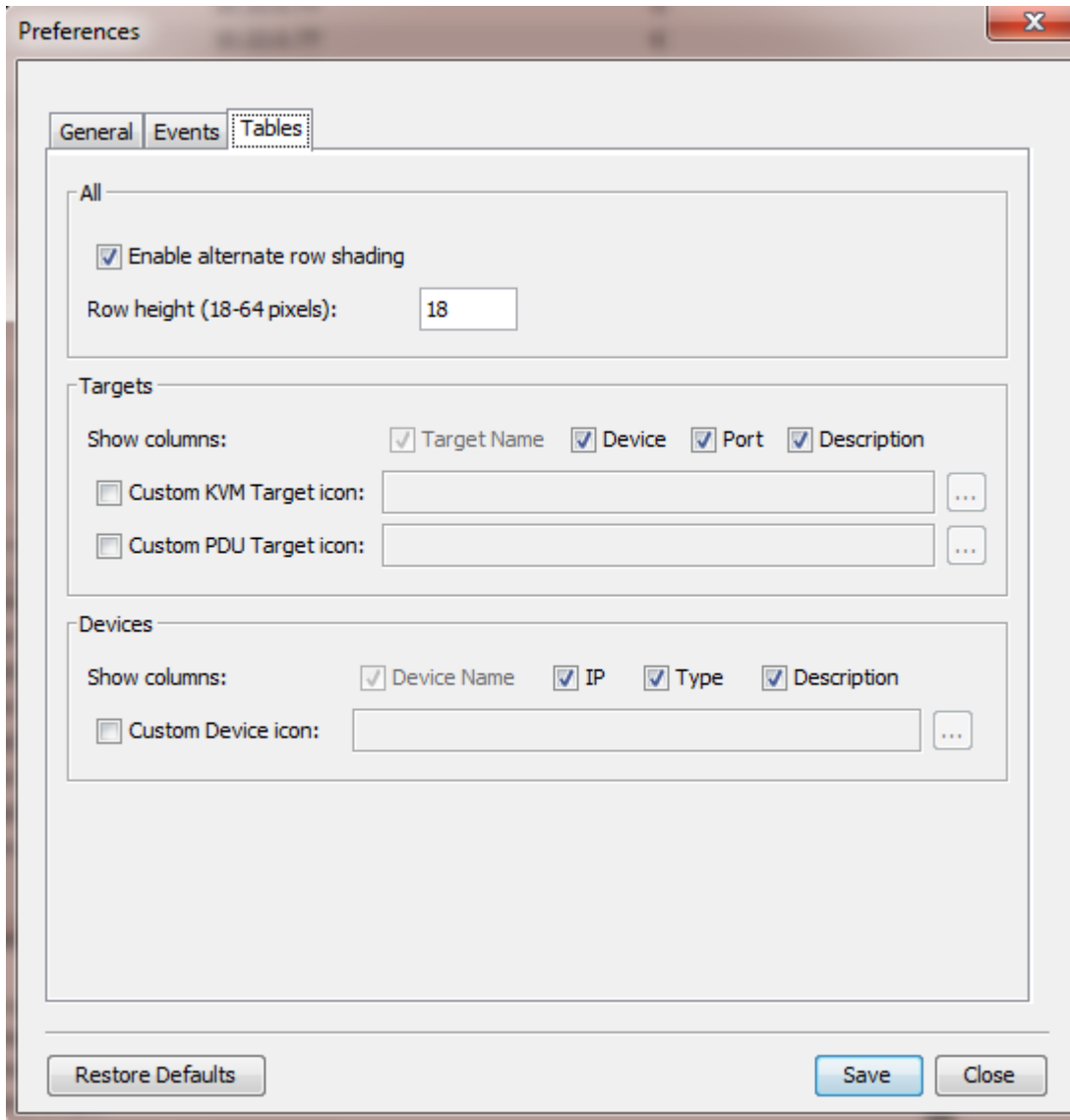
- General Tab:



- Events Tab:



- Tables Tab:



## Ping

A Device Ping utility is provided in the NetCommander-AXS. To use

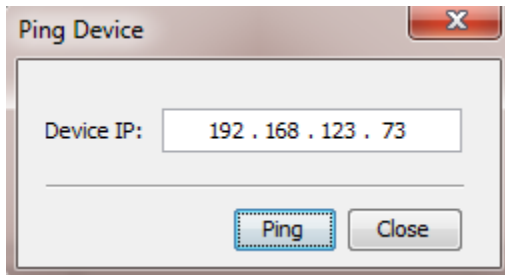
- Select a Device in the Devices table, and
  - Right-click and pick Ping menu item
  - Select Actions->Ping main menu item

Ping dialog is shown, initialized with the selected Device's IP address

- Select Actions->Ping main menu item

Ping dialog is shown, uninitialized

An image of the Ping dialog is shown below:



## Augmenting Supported PDU Devices

NetCommander-AXS provides for extending PDU device types that can be supported. In general, exercising this capability by end users is discouraged. Nevertheless, it is available, and is discussed below.

A file, pdu\_definitions.xml, can be found in the installation directory of NetCommander-AXS. This file defines the PDU model types that NetCommander-AXS supports.

The file can be edited, allowing for addition of new entries, including for PDUs from vendors other than Tripp Lite. (Make sure to save a back up prior to editing).

Below is an example of an entry for a Tripp Lite PDU model PDU3VSR. To add a new entry for a Tripp Lite PDU, simply copy and paste an existing entry, and edit the relevant fields, which would must include changes to:

device name,

description,

consolenumber,

and model.

For Tripp Lite devices, model represents the value the device will respond to for querying tlpDeviceModel SNMP variable.

```
<device name="Tripp Lite 24 Port PDU (PDU3VSR)" description="24 Port PDU"
manufacturer="Tripp Lite" model="PDU3VSR" consolenumber="24" mode="snmp">
    <snmp enabled="true"
sysobjectid="1.3.6.1.4.1.850.1">
```

```
        <poweron  
oid="1.3.6.1.4.1.850.100.1.10.2.1.4.#CONSOLE_PORT#" setvalue="2" />
```

```
        <poweroff  
oid="1.3.6.1.4.1.850.100.1.10.2.1.4.#CONSOLE_PORT#" setvalue="1" />
```

```
        <powercycle  
oid="1.3.6.1.4.1.850.100.1.10.2.1.4.#CONSOLE_PORT#" setvalue="3" />
```

```
        <powerstatus  
oid="1.3.6.1.4.1.850.100.1.10.2.1.2.#CONSOLE_PORT#">
```

```
        <powerstates>  
            <powerstate id="1"  
description="off"/>  
            <powerstate id="2"  
description="on"/>  
            <powerstate id="0"  
description="unknown"/>
```

```
        </powerstates>
```

```
    </powerstatus>
```

```
</snmp>
```

```
<monitor/>
```

```
</device>
```