User Manual

NetDirector AXS®

WARRANTY REGISTRATION

Register your product today and be automatically entered to win an ISOBAR surge protector in our monthly drawing!



www.tripplite.com/warranty

TRIPP·LITE

95 OVER YEARS
Manufacturing Excellence.

1111 W. 35th Street, Chicago, IL 60609 USA • www.tripplite.com/support

Copyright © 2019 Tripp Lite. All rights reserved.

FCC Information

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT: This equipment has been tested and found to comply with the limits for a Class B digital service, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. Any changes or modifications made to this equipment may void the user's authority to operate this equipment. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RoHS

This product is RoHS compliant.

User Information

Online Registration

Be sure to register your product at our online support center:

All Regions	https://www.tripplite.com/support/product-warranty-registration

Telephone Support

For telephone support, call this number:

International	1.773.869.1313 (intlservice@tripplite.com)
Domestic	1.773.869.1234 (techsupport@tripplite.com)

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Contents

FCC, CE Information ii
SJ/T 11364-2006. ii
User Information iii
Online Registration iii
Telephone Support iii
User Notice iii
About This Manual xii
Overview xii
Conventions xiii

Chapter 1.
Introduction
Overview 1
Features 2
Secure Centralized Management 2
Powerful Security 4
Server Management Features. 4
Requirements 5
Server Requirements 5
Client Requirements 6
Hardware Requirements 6
Operating Systems 6
Browsers 7
Device Requirements 7

Chapter 2.
NetDirector AXS Server Installation
Overview 9
Windows Version Installation 10
Before You Begin 10
Starting the Installation 10
Post-installation Check 15
Linux Version Installation 16
Before you Begin 16
Installing 17
Post-installation Check 18
Post-Installation Setup 18
Uninstalling the NetDirector AXS. 19
Uninstalling from a Windows System 19

Uninstalling from a Linux System 19
Upgrading the NetDirector AXS 20

Chapter 3.
Browser Operation
Logging In 25
The ND Interface 26
Screen Components 27
The Navigation Buttons 28
Tree View Considerations 29
Interactive Display Panel 29
Overview 29
Selecting List Items 30
Preferences 31
Web Options 32
Password 33

Chapter 4.
Port Access
Overview 34
Table Headings 35
Action Buttons 36
Filter 36
Launch Multiviewer 36
The Sidebar 37
Sidebar Characteristics 37
Sidebar Filter 38
Port Operation 39
ND Viewer 39
Web Access 40
Power ON / OFF 41
SSH / Telnet Session 41
Port Access Views 42
Port View 42
Target View 42
Device View 43
Department View 43
Location View 44
Type View 44
Favorites View 45
Adding a Favorite 45
Viewing a Favorite 46
Managing Favorites 47
User Preferences 48

Port Display 48
Alias 50

Chapter 5.
User Management

Overview 52
Accounts 53
Adding User Accounts 53
Managing User Accounts 57
User Information 57
Group Membership 57
Access Rights 58
Adding Device Access 58
Modifying Device Access 60
Removing Device Access 60
Managing Devices 60
Copy / Paste Access Rights 60
Deleting User Accounts 61
Unlocking User Accounts 62
Groups 63
Creating Groups 63
Adding Users to Groups 64
Removing Users from Groups 65
Access Rights 66
User Types 66
Members 67
Type Information 67
System Types 68
Custom Types 69
Authentication Services 70
NetDirector AXS Authentication 72
External Authentication Servers 73
Adding an External Authentication Server 73
Service Information 74
Deleting an External Authentication Server 76
Group Authorization 77

Chapter 6.
Device Management

Overview 79
Preliminary Procedures 80
Using VPN 80
Menu Structure 81
Devices 82
Devices 84
Adding a Folder or Device 85
Adding Folders 85
Adding Devices 85

Adding an Aggregate Device 90
Adding Ports to an Aggregate Device 93
Adding a Generic Device 94
Adding a Group Device 96
Modifying Devices 96
Deleting Devices 97
Deleting Unused Nodes 97
Detached Devices 98
Locking / Unlocking Ports 99
Locking / Unlocking Devices 99
Transfer Device Settings 100
Tools 101
Restoring Device Configurations 102
Default Access Rights 103
Device Sync 104
Sidebar Device Configuration 105
KVM Devices and Ports 105
Properties 105
Properties Page Action Buttons 107
Access Rights – KVM Devices 108
Adding Users or Groups to the Device User/Group List 108
Modifying a User's or Group's Rights 109
Deleting a User's or Group's Rights 109
Action Buttons 109
Access Rights – KVM Ports 110
Adding Users or Groups to the Port User/Group List 110
Modifying a User's or Group's Rights 111
Deleting a User's or Group's Access Rights 111
Action Buttons 111
Copy-Paste Access Rights 111
Device Configuration (For KVM Devices) 112
Port Configuration (For Cat5e KVM Devices) 113

Departments, Locations and Types 115
Adding a Department Location or Type. 115
Assigning Devices and Ports. 115
Modifying a Department, Location, or Type 116
Deleting a Department, Location, or Type. 116
Online Devices Information. 117
Unsupported Devices 118

Chapter 7.
System Management
Overview 120
This Server 121
Server Information. 121
Sessions 122
Server Settings 123
SMTP 123
NTP 125
Syslog. 125
Security 127
Login Policy 127
Lockout Policy 127
IP Filtering. 128
MAC Filtering. 128
Virtual Media Security Filters. 129
Certificate 130
Importing a Signed SSL Server Certificate 132
Tasks 133
Adding a Task. 134
Export Event Log. 135
Upgrade Selected Appliance Firmware 138
Backup Device Configuration/Account Information. 141
Export Device Log. 142
Editing a Task. 144
Deleting a Task. 144
Appliance Files. 145
Firmware Files. 145
Adding Firmware Files 145
Deleting Firmware Files 146

Chapter 8.
Logs
Overview. 148
NetDirector Logs. 148
ND Log Options. 150
Notification Settings. 151
Adding and Configuring Notification Users 152
Modifying Notification Configurations 153
Deleting Notification Configurations 153
Testing Event Notifications 153
Export Logs. 153
Import Logs. 155

Advanced Search 156
Device Log 157
Device Log Search 158
Device Log Options 159

Appendix A
Technical Information

. 160
.... .160
.... .162
Technical Support 163
International. 163
North America 163
Supported KVM Switches 164
Device ANMS Settings 164
VPNs. 165
Firewalls 166
ND Proxy Function 167
Name, Description and Range Parameters 168
Trusted Certificates. 171
Overview 171

About This Manual

This User Manual is provided to help you get the most from your NetDirector AXS system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Generally speaking, chapters 1, 3, and 4 are sufficient for basic users. The other chapters and appendixes are only required for specialized user types. For example, System Administrators, should read the entire manual; Device Administrators, chapters 6 and 8; User Managers, chapter 7. Custom user types will want to read the chapters appropriate to their assigned roles.

Overview

Chapter 1, Introduction, introduces you to the NetDirector AXS System. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, NetDirector AXS Server Installation, provides step-by-step instructions for installing the NetDirector AXS on a Windows and Linux system.

Chapter 3, Browser Operation, explains how to log into the NetDirector AXS with a browser, and describes how to work with the NetDirector AXS' browser GUI interface.

Chapter 4, Port Access, shows how to access and control the KVMs that will be managed over the NetDirector AXS network.

Chapter 5, User Management, describes how to: add, modify and delete user accounts; create user groups and assign users to them; specify device access rights for users and groups; and specify the user authentication method.

Chapter 6, Device Management, explains how to add, configure, and organize the KVMs that will be managed over the NetDirector AXS network.

Chapter 7, System Management, provides an overview of the NetDirector AXS organizational concept, and demonstrates how to deploy, configure, and manage the NetDirector AXS server on your installation.

Chapter 8, Logs, explains the NetDirector AXS' logging function and how to access, filter, and search the various logs that are kept by the NetDirector AXS.

Appendix A, Technical Information, provides technical as well as troubleshooting information.

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
⚠	Indicates critical information.

Product Information

For information about all Tripp Lite products and how they can connect without limits, visit www.tripplite.com or contact Tripp Lite directly.

International	1.773.869.1313
Domestic	1.773.869.1111

Chapter 1
Introduction

Overview

The NetDirector AXS provides single portal, single login, secure, centralized, access, administration and management of your entire network – local and worldwide – anywhere; anytime.

The NetDirector AXS offers a single, integrated browser-based interface to manage your KVM and the devices connected to them. Users no longer need to learn the interface for each individual device, making system management easier and more efficient.

By consolidating the management of your Tripp Lite KVMs, the NetDirector AXS allows every device to be securely accessed and controlled by means of a single IP address. Servers and network equipment are integrated into a single tree view, making the NetDirector AXS ideal for enterprises with data centersand branch offices, located in several locations.

Recognizing the broad spectrum of computing environments, the NetDirector AXS Java software implementation allows it to work with Sun Java Runtime Environment (JRE) enabled operating systems – ensuring multi-platform integration and mutual opperability.

Features

Secure Centralized Management

- Complete control of your enterprise – consolidates the management of all Tripp Lite KVMs
- Single portal, single sign-on, single IP address to securely access every device on the installation
- All devices are integrated into a single tree view for centralized access, administration, and management of a worldwide network from anywhere at anytime
- Multiplatform installation support – Windows / Linux
- Multiplatform client support (Windows, Mac OS X, Linux, Sun)
- Multi-browser support – Internet Explorer, Chrome, Firefox, Safari, Opera, Mozilla, Netscape
- Email notification of specified system events
- Automatic scheduling of system, configuration, and maintenance tasks
- Logging and auditing of system events for the NetDirector AXS and supported KVMs
- Session logs provide serial device keystroke history
- View, manage, and terminate active user sessions in real time
- User level management identification
- Browser-based GUI offers a multilanguage interface to minimize user training time and increase productivity

- Flexible logging and report options
- Integrates all access rights – Web, SSH/Telnet, VNC/RDP, IPMI/SPM, KVM to target device
- Panel DynaArray – view the output of multiple ports in individual panels on the same screen
- Web-based wizard to quickly install supported KVMs
- Advanced search function for log entries
- Strong session management/Integrates multi-session
- Data export /import to remote server or local in real time or on schedule. AES/DES encryption support for data export
- OOBC, PAP and CHAP authentication
- IPv6 support
- NTS support – allow your device to get the accurate time from a server that the administrator assigns

Powerful Security

- Powerful security features include both internal and external authentication – external authentication support includes LDAP, LDAPS, Kerberos, Active Directory, RADIUS, TACACS+, and NT Domain
- Option to force users of all ND managed devices to be authenticated through the ND – users cannot log in to the devices directly
- Compliant with the X.509 Digital Certificate Standard
- Supports TLS 1.2 data encryption and RSA 2048-bit certificates to secure users logging in from browsers
- Flexible session time-outs
- Configurable user and group permissions for server access and control
- Supports password protection, SAS 70 compliance for configurable amount of failed login attempts and user ID lock out parameters
- Devices can identify themselves by Name, MAC address, or IP in the browser
- IP and MAC filtering
- Private CA support

Server Management Features

- BIOS level support
- Flexible encryption design allows users to choose any combination of 56-bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4, or Random for independent KB/Mouse, video, and virtual media data encryption
- Virtual Media – supports CAC/Smart Card readers, fingerprint readers, DVD/CD drives, USB mass storage devices, PC hard drives and ISO images
- Exit Macro support
- Mouse DynaSync – automatically synchronizes the local and remote mouse movements
- Panel Array Mode – simultaneous monitoring of the video output of the installations' servers
- Scalable Video Display

Requirements

Server Requirements

Systems that the NetDirector AXS server will be installed on should meet the following requirements:

- Hardware Requirements
  - CPU: Pentium 4, 2.60 GHz or higher
  - Memory: At least 512MB (1GB or more recommended)
  - Hard drive: 500MB or more free space
  - Ethernet: At least 1 Ethernet adapter (100Mbps or higher) – Giga LAN recommended
- Operating System Requirements
  - Windows: 2000, XP, 2000 Server, Server 2003, Server 2008, or Windows Vista with Java Runtime Environment (JRE) 6, Update 11, or higher (with the latest service package for each installed)
  - Linux (with Java Runtime Environment (JRE) 6, Update 11, or higher)
    - Red Hat Enterprise Linux V. 4
    - Novell SUSE Enterprise Server 9 and 10

Client Requirements

Hardware Requirements

- CPU: We recommend that the computers used to access the switch have at least a Pentium 4 2GHz processor, with their screen resolution set to 1024 x 768.
- Memory: At least 512MB (1GB or more recommended)
- Ethernet: At least 1 Ethernet adapter – 10Mbps or higher – 100Mbps recommended
- Browsers must support 128 bit SSL encryption.
- For the browser-based Java Applet Viewer the latest version of the Java Runtime Environment (JRE) must be installed.
- At least 205MB of memory must be available for the first viewer after logging in from the browser and 100MB for each additional viewer that is opened, thereafter.

Operating Systems

- Supported operating systems for client workstations that connect to the NetDirector AXS are shown in the table, below:

OS		Version
Windows		2000 and higher
Linux	RedHat	7.1 and higher
	Fedora	Core 2 and higher
	SuSE	9.0 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	4.2 and higher
	Sun	Solaris 8 and higher

- Supported operating systems for users that log into the NetDirector AXS include Windows 2000 and higher, and those capable of running the Java Runtime Environment (JRE) 6, Update 11, or higher.

Note: The Windows 2000 Client does not support the WinClient Viewer.

Browsers

Supported browsers that log into the NetDirector AXS include the following:

Browser		Version
IE		6 and higher
Chrome		8.0 and higher*
Firefox	Windows	3.5 and higher
	Linux	3.0 and higher
Safari	Windows	4.0 and higher
	Mac	3.1 and higher
Opera		10.0 and higher
Mozilla	Windows	1.7 and higher
	Sun	1.7 and higher
Netscape		9.0 and higher

Note: For newer versions of Chrome, you may need to enable the NPAPI (Netscape Plugin Application Programming Interface) manually by keying the command "chrome://flags/#enable-npapi" in the URL bar. Or you can go to Java.com (https://java.com/en/download/faq/chrome.xml) for more details.

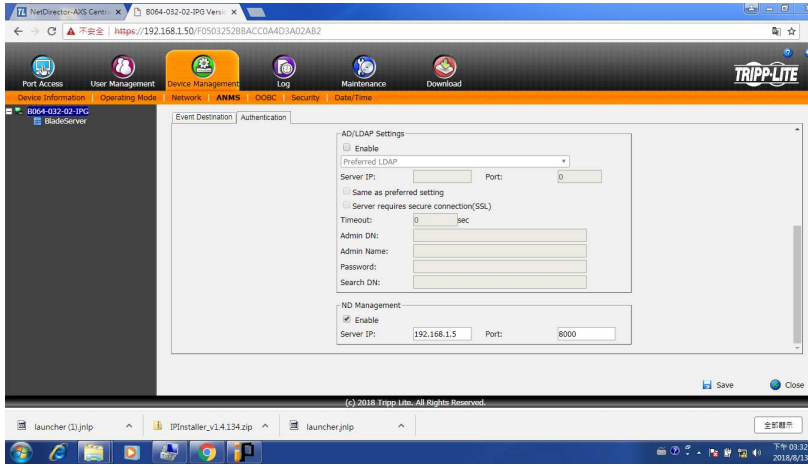
Device Requirements

All Tripp Lite IP products must be at a firmware level that contains the NetDirector AXS Management function, and the ND Management function must be enabled. It is suggested that Tripp support be contacted for correct firmware versions for the targeted KVM. The latest version of the relevant firmware from our Website may be downloaded and installed, if necessary. For details on upgrading the firmware see *Upgrade Selected Appliance Firmware*, page 138.

Note: 1. Devices must be configured to communicate on the same port that you configure for the NetDirector AXS's Device Port (see *Device port*, page 13).

2. To allow authorization for the KVM over IP switch through a ND (NetDirector AXS) server, check Enable and fill in ND Server's IP

address and Service port in appropriate fields. You can use the IPv4 address, the IPv6 address or the domain name in the ND Server IP field.



Chapter 2
NetDirector AXS Server Installation

Overview

Recognizing the increasing importance of Linux in the server environment, the NetDirector AXS system makes the NetDirector AXS's management services available on both the Windows and Linux platforms. This chapter describes how to install the NetDirector AXS server on each of them.

Windows Version Installation

Before You Begin

Before running the installation program, make sure that Sun's Java Runtime Environment (JRE) 6, Update 11, or higher has been installed on your system. If not, you will first need to download and install it. You can find the latest version on Java's official web site:

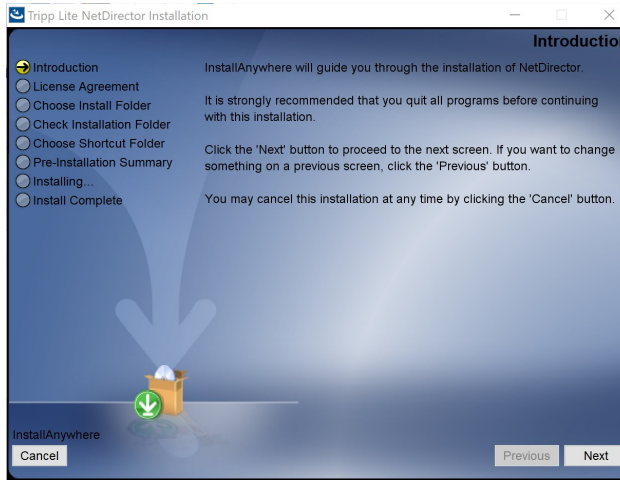
```
http://java.com
```

After JRE has been installed on your system, you will be ready to install the NetDirector AXS program.

Starting the Installation

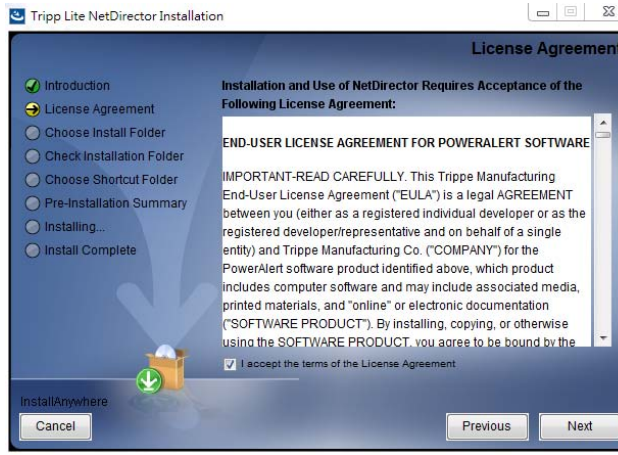
To install NetDirector AXS on a Windows system, do the following:

1. (Download NetDirector AXS from Tripp Lite website.)
2. Go to the folder where (*NetDirAXS.exe)* located, and execute it. A screen, similar to the one below, appears:



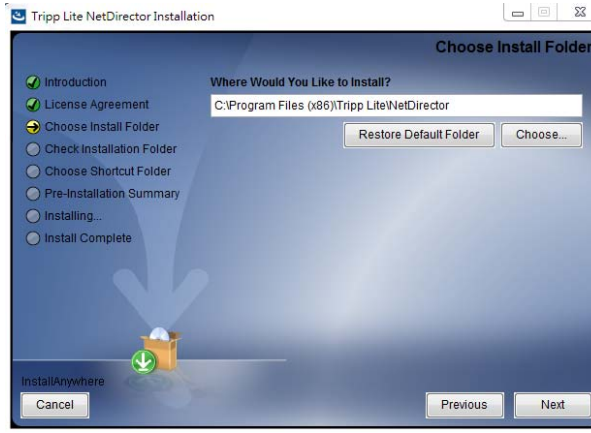
Click **Next** to move on.

3. In the screen that comes up, read the *License Agreement*, then click to enable the *I accept...* radio button:

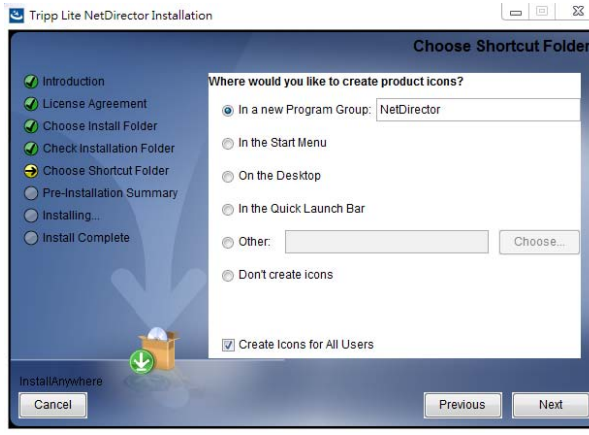


4. Click **Next** to continue.

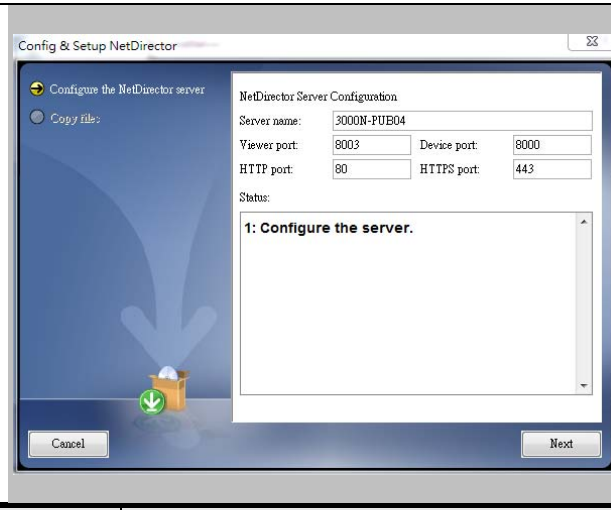
5. In the *Choose Installation Folder* dialog box, specify the NetDirector AXS's installation folder. If you don't want to use the default entry, click **Choose...** to browse to the location that you want, then click **Next** to continue.



8. In the *Choose Shortcut Folder* dialog box, click one of the radio buttons to specify where you would like to create product icons, then click **Next** to continue.



9. In the Configuration dialog box that comes up, fill in the fields according to the information provided in the table, below.



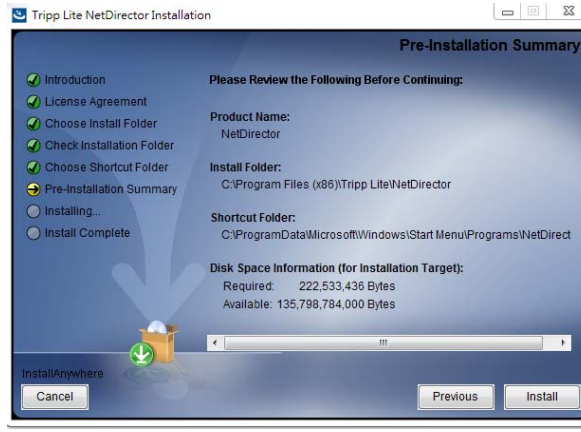
Heading	Explanation
Server name	The dialog box presents the default name for the server – as defined in the Windows *Computer Name* setting. You can choose a different name to identify the server on the NetDirector AXS' installation, if you wish. The name can be from 2–32 bytes in any supported language. **Note:** 1. The following characters may not be used: **" ' ** 2. This name is only for NetDirector AXS server purposes – it doesn't change the actual computer name.
Device port	The port that the NetDirector AXS server uses to communicate with the devices (Tripp Lite IP products) on the installation. The default is 8000. Each NetDirector AXS can have a separate Device port number, but in order to communicate with the devices connected on its network segment, those devices must be configured to use the same port as the one set here.
HTTP port	The port that the NetDirector AXS server uses for web communication. The default is 80. If you use a different port, users must specify the port number in the URL of their browsers.
HTTPS port	The port that the NetDirector AXS server uses for secure web communication. The default is 443. If you use a different port, users must specify the port number in the URL of their browsers.

10. After the fields have been filled, click **Next** to continue.

Note: You can change any of these settings following the installation. See *Server Information*, page 121, for details.

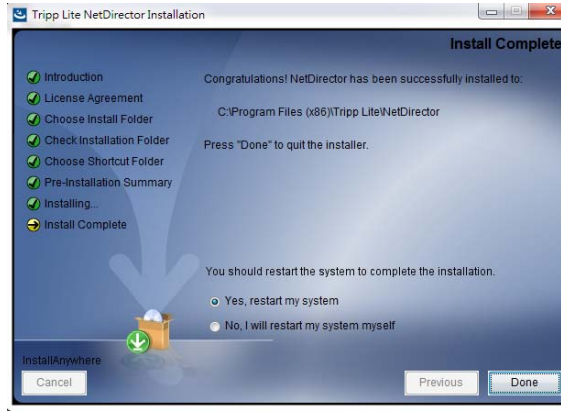
11. The dialog box changes to inform you that files are being copied to the installation folder. Once the files have been copied, click **Continue** to move on.

12. The *Pre-Installation Summary* screen appears:



If you wish to change anything, click **Previous** to go back, If the information is correct, click **Install**.

13. When the installation utility brings up a screen informing you that the installation has completed successfully, click **Done** to exit the installer.

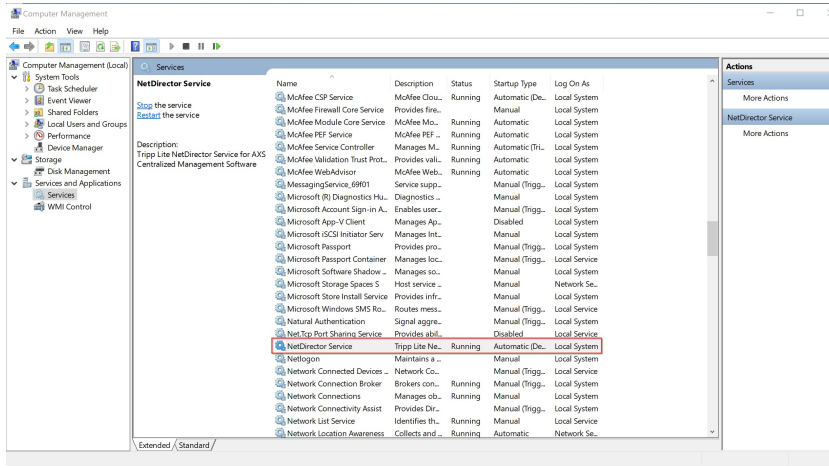


14. At the completion of the installation, a NetDirector AXS entry is created in the Windows *Start* menu:

Post-installation Check

After the installation completes successfully, the NetDirector AXS program starts automatically (and starts automatically with every bootup).

To check that the NetDirector AXS has started, navigate through the following folders: Control Panel → Administrative Tools → Services. Look down the list to the NetDirector AXS entry. If the NetDirector AXS is running it will appear in the services list. You should see a screen similar to the one, below:



The entry for the Status field should say *Started*. If it does not, right click anywhere on the NetDirector AXS entry line and select **Start** from the pop up menu.

Linux Version Installation

Before you Begin

The procedure for installing NetDirector AXS on a Linux system is similar to that for Windows, but there are Java considerations to take note of first.

- If Java isn't already installed on your system, you will need to download it from the Java web site:

  ```
  http://java.com
  ```

  Installation instructions are provided on the Java download page.

- Some Linux distributions install an earlier version of Java than the JRE 6, Update 11, or higher required by the NetDirector AXS program. To check the Java version on your system, open a terminal and enter the following:

  ```
  java -version
  ```

  If the version it displays refers to a Java version that is earlier than JRE 6, Update 11, you must install a JRE version that is Version 6, Update 11 or higher. (See the previous point regarding downloading and installing Java.)

- Make sure your PATH and JAVA_HOME environment variables point to the new version in your */root/.bash_profile* file. For example:

  ```
  JAVA_HOME=/usr/java/jre1.6.0_0-b11
  PATH=$JAVA_HOME/bin:$PATH:./
  BASH_ENV= $HOME/.bashrc
  USERNAME= "root"
  export JAVA_HOME PATH BASH_ENV USERNAME
  ```

- Even after you install an appropriate Java version and set the new PATH and JAVA_HOME environment variables, the distribution may still not recognize the new version and continue to use its original Java version. If the problem exists on your installation, correct it by doing the following:

  1. Copy the NetDirAXS.bin file from the Tripp Lite website to a folder on your hard disk.
  2. Open a terminal and go to the directory where the *NetDirAXS.bin* file is located.
  3. Enter the following commands:

     ```
     export LAX_DEBUG=1
     sh NetDirAXS.bin
     ```

     Note: If the installation program starts, cancel it.

4. In the screen output, look for the line (it will be in bold) that starts:

   ```
   Using VM.........
   ```

   to see which Java your distribution is defaulting to.

5. If the *Using VM* entry shows a path to a file named *java* in the old Java version directory, go to that directory and either delete the *java* file or rename it.

6. Log out and log back in.

Installing

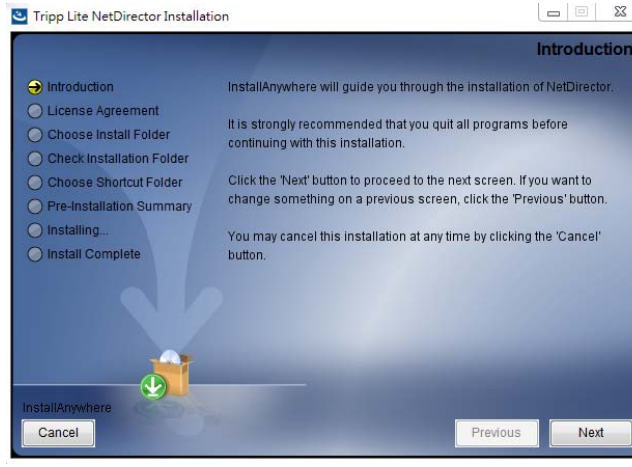
After making sure that the appropriate version of the JRE has been installed, do the following:

1. Download from Tripp Lite website.
2. Go to the folder where *NetDirAXS.bin* is located, and run it.

Note: 1. You must run the installation program as the root user.

2. Make sure that the installation file has executable permissions
3. For some versions of Linux, the program must be run in a terminal.

A screen, similar to the one below, appears:



Click **Next** to move on.

4. From here, the installation procedure is the same as the one for Windows. Refer to the Windows installation procedure (see page 10), for details on how to proceed.

Post-installation Check

- After the installation completes successfully, the NetDirector AXS program starts automatically (and starts automatically with every bootup).

  To check that the NetDirector AXS has started, start, stop, and restart, the service by issuing the following commands (as root) from a terminal console:

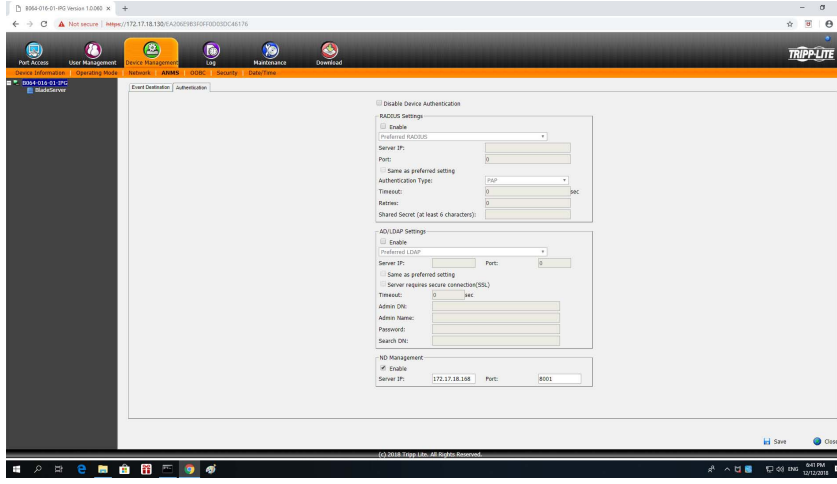
  - /etc/init.d/netdirectorservice start#to start the service
  - /etc/init.d/netdirectorservice stop#to stop the service
  - /etc/init.d/netdirectorservice restart#to restart the service
  - /etc/init.d/netdirectorservice status#to check the service status

- To check on the Java version your system is running, do the following:

  1. Open the *Start* menu.
  2. Navigate to the NetDirector AXS entry (Programs → NetDirector AXS) , and select **Java Version Checker**.

ND Management Settings

To allow authorization for the KVM over IP switch through a ND (NetDirector AXS) server, check Enable and fill in the ND Server's IP address and Service port in the appropriate fields. You can use the IPv4 address, the IPv6 address or the domain name in the ND Server IP field.



Uninstalling the NetDirector AXS

Uninstalling from a Windows System

To uninstall the NetDirector AXS from a Windows system, do the following:

1. Open the *Start* menu.
2. Navigate to the NetDirector AXS entry (Programs → NetDirector AXS) , and select **Uninstall** NetDirector AXS

Note: The removal program does not remove a number of the NetDirector AXS files and folders that were created duringoperation. For a complete removal (necessary if you plan on reinstalling), you must remove them yourself from the location that the NetDirector AXS was installed at (the default folder is C:\NetDirector AXS).

Uninstalling from a Linux System

To uninstall the NetDirector AXS from a Linux system, as root, execute the following command:

```
/install-path/Uninstall_NetDirectorAXS/Uninstall_NetDirectorAXS
```

Where */install-path/* represents the path anddirectory that you specified for the NetDirector AXS's location when you installed the program.

Note: The removal program does not remove a number of the NetDirector AXS files and folders that were created during installation. For a complete removal (necessary if you plan on reinstalling), you must remove them yourself. The default is /home/NetDirector AXS

Upgrading the NetDirector AXS

If the NetDirector AXS program has already been installed, it is not necessary to perform a full install. You can upgrade to the latest NetDirector AXS version by running the NetDirector AXS-Upgrade program:

Please see www.tripplite.com for details

New versions of the Upgrade Program are put up on our website for download as they become available. Check the website to get the most up-to-date version.

Preliminary Steps

These steps make sure that the installation database is at the most current level across all of the NetDirector AXS units. If a problem should occur after the upgrade, you can use the backup created with them to restore the database to its latest working level.

We recommend you take the following backup steps on each NetDirector AXS unit before you begin.

1. Replicate the database of each of the secondaries; use *Run Now* for the schedule setting.
2. After replication completes; go back and set the schedule to a time that will not take place during the upgrade time (next week, next month, etc.).

When you run the upgrade program, simply follow the installation Wizard to complete the procedure.

Chapter 3
Browser Operation

To ensure multi-platform operability, access to the NetDirector AXS is available through most standard web browsers. Once users log in and are authenticated, the NetDirector AXS's browser GUI comes up. This chapter explains the login procedure, and describes the NetDirector AXS's browser GUI components.

Logging In

To log into the NetDirector AXS, do the following:

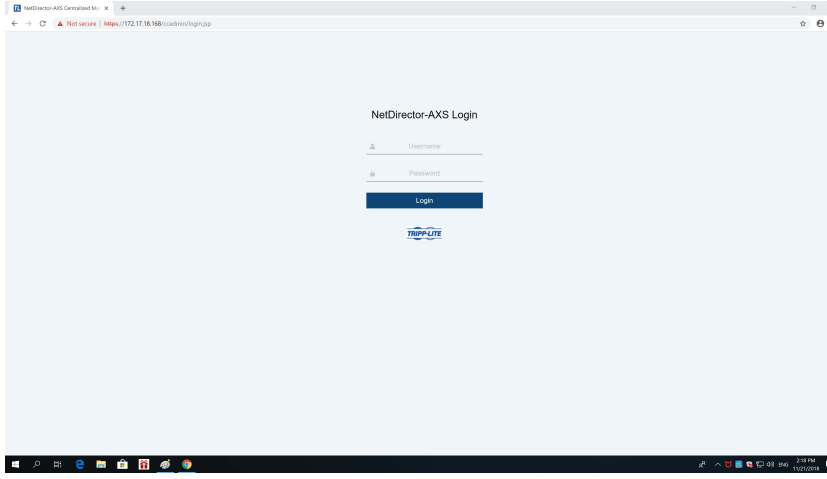
1. Open the browser and specify the IP address of the NetDirector AXS in the browser's URL location bar.

   Note: If the system administrator has configured the HTTP or HTTPS port setting as something other than the NetDirector AXS defaults, you must include **http://** or **https://** before the IP address, and specify the port number along with the IP address. For example:

   ```
   http://192.168.1.20:8082
   ```

   Where *8082* is the http port number, and a colon is inserted between it and the IP address.

2. If any Security Alert dialog boxes appear, accept the certificate – it can be trusted. See *Trusted Certificates*, page 171 for details. After a moment, the Login page appears:

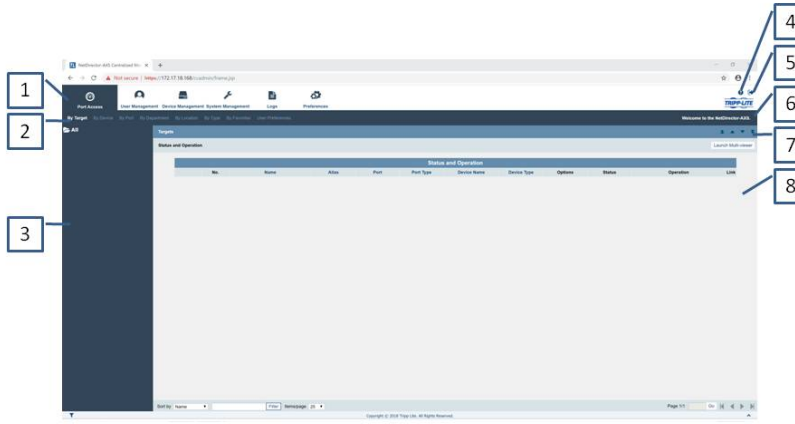


3. Provide your NetDirector AXS Username and Password*, then click **Login**.

Note: There is a pre-installed system administrator account that can be used to log in for the first time to begin creating users and groups, adding devices, configure the system, etc. The Username for this account is *administrator*; the password is *password*. For security purposes, we strongly recommend you change this to something unique. See *Managing User Accounts*, page 57 for details.

The ND Interface

After you have successfully logged in, the ND web page appears:



Screen Components

The NetDirector AXS's screen components are described in the table, below:

No.	Item	Description
1	Tab Bar	The tab bar contains the NetDirector AXS's main operation categories. The items that appear in the tab bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
2	Page Menu Bar	The page menu bar contains operational sub-categories that pertain to the item selected in the tab bar. The items that appear in the menu bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
3	Sidebar	The Sidebar provides a tree view listing of items that relate to the various tab bar and menu bar selections. Clicking an item in the Sidebar brings up a page with the details that are relevant to it.
4	About	About provides information regarding the current version of the NetDirector AXS.
5	Logout	Click this button to log out your NetDirector AXS session.
6	Welcome Message	If this function is enabled (see *Preferences*, page 31), a welcome message displays here.
7	Navigation Buttons	These buttons move you through the Sidebar. Their usage is discussed in the next section of this chapter.
8	Interactive Display Panel	This is your main work area. The screens that appear reflect your menu choices and Sidebar item selection. The use of this panel is discussed later in this chapter – see *Interactive Display Panel*, page 29.

The Navigation Buttons

The navigation buttons move you through the items in the Sidebar as follows:

Button	Action
	Moves to the item in the tree that is one level out and one step up from the current selection (its parent item).
	Moves to the item in the tree that is on the same level of depth and one step up from the current selection (its sibling item).
	Moves to the item in the tree that is on the same level of depth and one step down from the current selection (its sibling item).
	Moves to the item in the tree that is one level in and one step down from the current selection (its child item).

One of the advantages of using the navigation buttons instead of clicking on an item in the Sidebar lies in the fact that you stay on the same Panel Menu page as you move from item to item.

Note: When you make a menu choice, a Panel Menu bar with further choices appears in the Interactive Display Panel. See *Interactive Display Panel*, page 29, and the table on page 30.

Note: If an item's icon contains a question mark, it indicates there is a mismatch between the device's information and the information for it stored in theNetDirector AXS's database. See *Update*, page 107, for information on resolving the problem.

Tree View Considerations

- Only items a user is authorized to access appear in the Sidebar tree view.
- A plus (+) sign in front of an item means that there are additional items nested inside of it. Click the plus sign to expand the view and show the nested items.
- The plus sign changes to a minus sign (-)when an item is expanded. Click the minus sign to collapse the view and hide the nested items.
- For devices, if the device is on line, its icon is in color; if it is off line, its icon is gray.

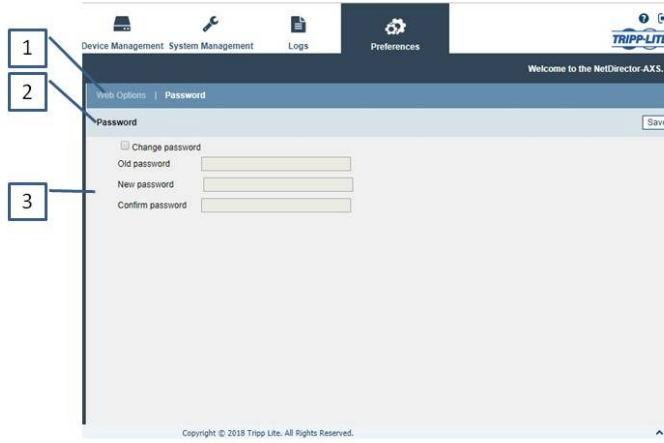
Note: User's can configure the way devices and ports display in the Sidebar tree view. See *User Preferences*, page 48, for details.

Interactive Display Panel

Overview

The Interactive Display Panel (also referred to as the main panel) is your main work area. The screens that appear reflect your menu choices and Sidebar item selection. The reason it is called an interactive display panel, is that in addition to displaying the contents of your menu choices, it is also a work area where you can make configuration settings and perform actions on selected devices.

An explanation of a typical interactive display panel is given below:

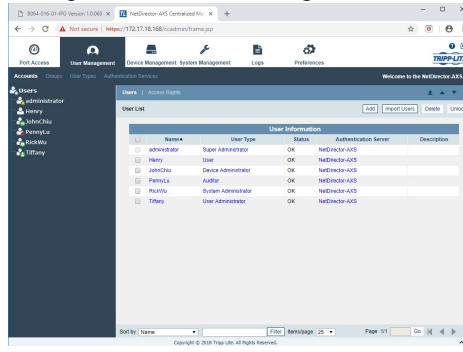


(Continued from previous page.)

No.	Item	Description
1	Panel Menu Bar	◆ Refines the menu category into smaller related groupings. ◆ If there are secondary Panel Menu pages, hovering over the Panel Menu title causes a popup menu to appear. Click on the menu item to go to the desired secondary page. ◆ The items that appear in the Panel Menu bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
2	Panel Menu Title Bar	◆ Describes the Panel Menu category. ◆ If there are secondary Panel Menu pages, an arrow icon indicates so. Click the Down-Arrow icon to go to the next page in the sequence; click the Up-Arrow icon to go to the previous page in the sequence.
3	Action-Input Area	A button or input box displays here directing you to take an action (Save, Delete, Add, Next, etc.), with regard to the current page.

Selecting List Items

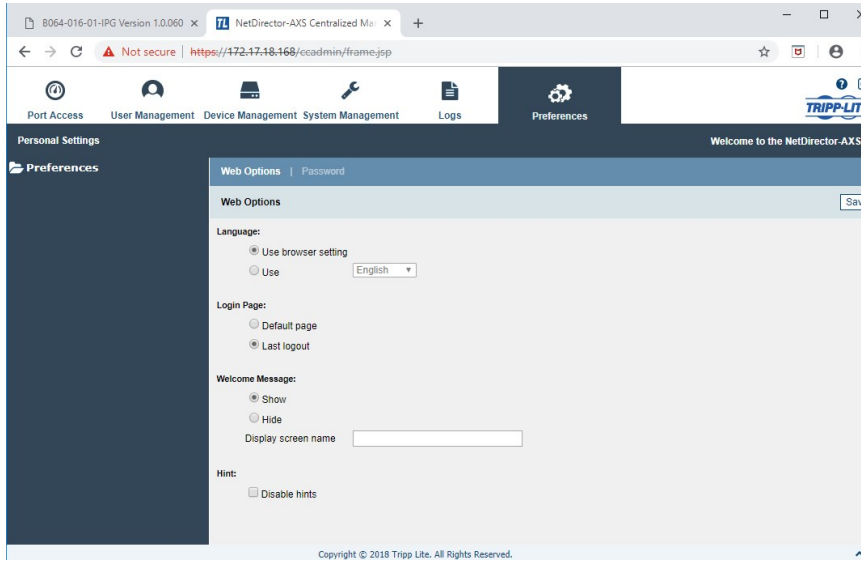
Many of the pages displayed in the Interactive Display Panel contain a list of items (devices, users, groups, configuration files, etc.), that you will select to perform some operation on. For example:

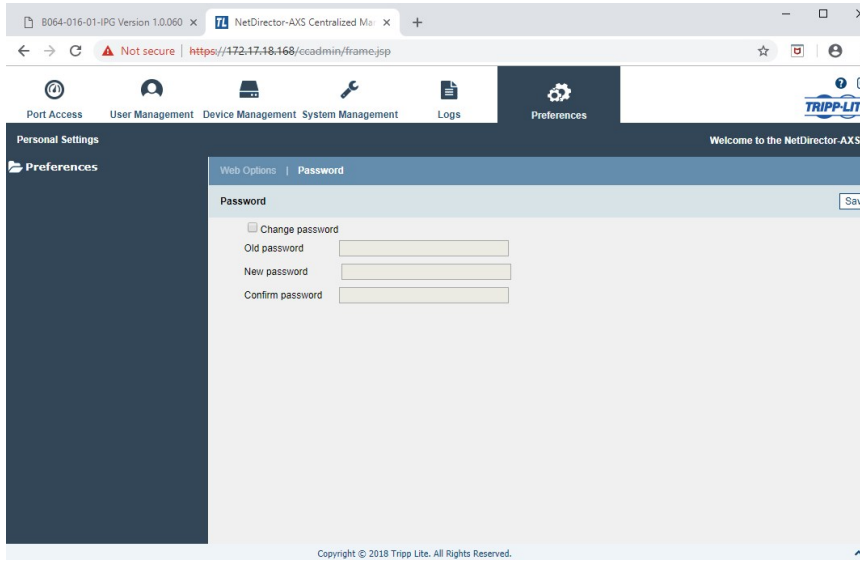


- You can select an individual item by clicking to put a check in the checkbox in front of its name.
- You can select a group of items by clicking to put a check in the checkbox in front of each of their names.
- You can select all of the items by clicking to put a check in the checkbox at the top of the column.

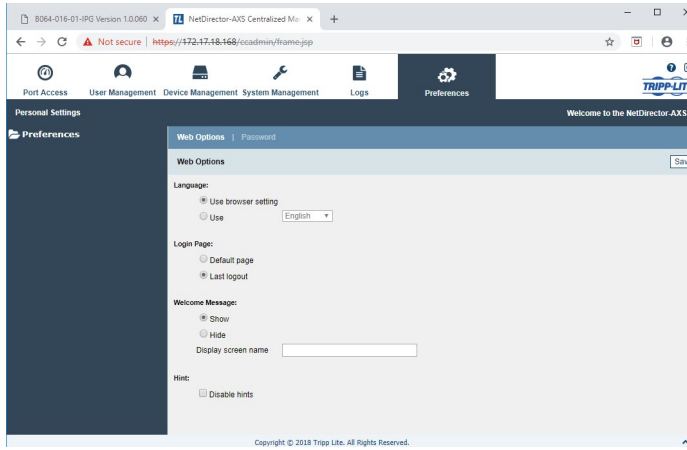
Preferences

Users can set individual preferences for their browser sessions by clicking the *Preferences* tab on the Tab Bar. The Interactive Display Panel opens to the default page – Web Options. The Panel Menu bar shows the available categories: *Web Options* and *Password*.





Web Options



- For *Language*:
  - Click the **Use Browser Settings** radio button to have the NetDirector AXS's pages display in the same language that your browser is set to.

    Note: If your browser is set to a non-supported language, the NetDirector AXS looks to what your server's operating system is set to. If the operating system is set to a supported language it will use that language to display its pages. If the operating system is set to a non-supported language, the NetDirector AXS defaults to English.

  - Click the **Use** radio button to drop down a list of supported languages and have the NetDirector AXS's pages display in the language you select.

    Note: The language selected here, if different from the browser's setting, will only take effect after login. The login page will follow the sequence described in the note for *Use Browser Settings*.

- For *Login Page*: You can choose to have the NetDirector AXS open to the default page when you log in – which is the first page of the first available tab on the Tab Bar – or you can choose to have the NetDirector AXS open to the page you were on the last time you logged out.

- For *Welcome Page*:
  - If you want the Welcome Message to appear on screen, select **Show**; if you don't want it to appear, select **Hide**.
  - If you want a Screen Name to appear with the Welcome Message, key it into the *Display screen name* text box.

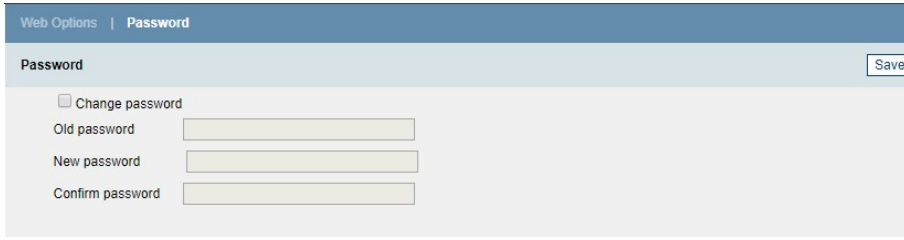
Note: 1. This provides a way of changing the screen name specified in your User Account. When you change the name here, the Screen Name entry in the User Accounts settings will automatically change to what you specify here (see *Adding User Accounts*, page 53).

2. The Screen Name will not display unless you choose to *Show* the Welcome Message.

- To disable mouse-over hints from appearing, click to put a check mark in the *Disable hints* checkbox.

When you have made your choices, click **Save**.

Password



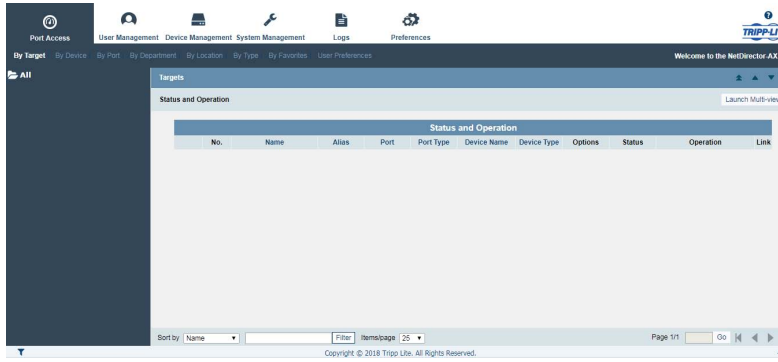
If you wish to change your password, do the following:

1. Check **Change Password**. This enables the password input fields.
2. Key in your old password in the *Old password* field.
3. Key in your new password in the *New password* field.
4. Key in your new password again in the *Confirm password* field.
5. Click **Save**.

Chapter 4
Port Access

Overview

The *Port Access* page is used to access and control the devices and ports that are managed over the NetDirector AXS network. The page's Menu Bar provides different organizational views of those items, as shown in the screenshot, below:



Click the view on the Menu Bar that you want to see the items organized by. From there, you can operate the items as described in the sections that follow.

Note: If no access rights have been assigned to a user, the Port Access tab and page do not display – even for System Administrators.

Table Headings

An explanation of the column headings is provided in the table, below.

Note: 1. The headings at the top of the table don't all appear for each view. Which ones appear vary depending on the view selected.

2. You can change the sort order of the items by clicking on the column headings.

Heading	Explanation
Name	The name given to the port when it was added to the NetDirector AXS installation.
Alias	If you gave the port an alias, the alias name appears here.
Port	The port's port number on the device it belongs to.
Port Type	Indicates the kind of device that the port belongs to.
Device Name	The name of the device that the port belongs to.
Device Type	The type of device that the port belongs to .
Options	◆ For KVM ports, indicates the port's *Access Mode*. See *Mode*, page 114, for details. ◆ This item is blank for Target device ports.
Status	◆ For KVM ports, indicates whether the port is online or offline.
IP Address	For physical devices – the device's IP Address displays here.
MAC Address	For physical devices – the device's MAC Address displays here.
Operation	The default action for accessing the device/port appears in this cell. ◆ Click the arrow at the right of the table cell to see what other actions (if any), are available. ◆ Click your choice to open a session for the device/port. The various device/port operation choices are described in the *Port Operation* section that follows.
Link	Click to go to the device's Device Management → Port page.

Action Buttons

There are two buttons on the main panel: *Filter* at the bottom of the page, and *Launch Multiviewer* at the top right of the page.

Filter

Filter allows you to control which items appear in the main panel list. Key in a string and click **Filter** (or tap **[Enter]**). Only items that have that particular string in their names display in the list.

For example, if *TD* is your string, only items with names containing TD, such as *TD-AGG-01*, will be displayed.

Sort by: To sort the devices displayed in the main panel, use the **Sort by** menu to select a criteria to sort by: *Name*, *Alias*, *Type*, *IP Address*, or *MAC Address*. You can use the Sort by feature with or without applying the filter.

Items/Page: Use this drop down menu to select how many devices you want to display on the page. Options are: *25*, *50*, *75*, *100*, and *400*. To prevent extremely slow loading, the maximum number of devices that can be displayed per page is 400.

To clear the filter and bring back the complete list, erase the contents of the input box and click **Filter**, again.

Launch Multiviewer

If you want to launch viewers for more than one port at a time, check the checkbox in front of the name of the ports you want to access, then click **Launch Multiviewer**.

The Sidebar

Devices, ports and outlets that have been configured on the NetDirector AXS are listed in a tree structure in the Sidebar at the left of the screen:



Sidebar Characteristics

The characteristics of the Sidebar tree structure are the following:

- Users are only allowed to see the devices and ports that they have access permission for.
- Ports and child devices can be nested under their parent devices.
  - Click the + in front of a device to expand the tree and see the ports nested underneath it. Click the - to collapse the tree and hide the nested ports.
  - For faster port access the tree is collapsed and must be expanded for node access. For every 2000 nodes the tree will be divided into a separate folder, so that the page loads faster.
- Switches and ports that are online have their monitor screen icons in Green; the monitor screens are Gray for devices and ports that are offline.
- Clicking an item in the tree brings up its *Status and Operation* page.

- Double clicking an active device or port opens the viewer for it.
- Right clicking an active device or port opens a pop-up that allows you to select a viewer to access it with (see *Port Operation*, page 39, for details).

Sidebar Filter

Filter allows you to control the number and type of devices and ports that display in the Sidebar. When you click the funnel icon at the bottom left of the Sidebar panel it brings up the Filter dialog, which looks similar to the image, below:



The meanings of the choices are explained in the following table:

Choices	Explanation
All	This is the default view. With no other filter options selected, all of the devices and ports and that are accessible to the user are listed in the Sidebar. Drop down the list box to see all of the available choices and select one of them instead of All. Only the items that match your selection display in the tree.
Online	If you enable *Online* (by putting a check in the checkbox) only items that are online display in the tree.
Search	If you key in a search string and click **Search**, only device and port names that match the search string display in the tree. Wildcards (? and *) are acceptable, so that more than one item can show up in the list. For example, if you key in **Web***, both Web Server 1 and Web Server 2 show up in the list.

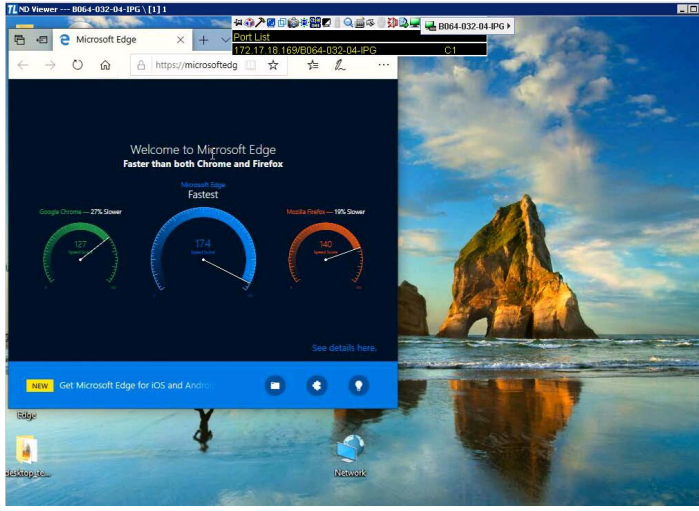
To dismiss the Filter dialog, click the downward-pointing chevron at the bottom left of the Sidebar panel.

Port Operation

Depending on the item chosen, various port operation methods are available to access and control it. Click the arrow at the right of the Operation cell to select an operation method, as explained in the following sections.

ND Viewer

Clicking ND Viewer opens a KVM or Serial viewer directly to the device running on the selected port. It is just like what you would see if you logged into the device directly and then selected that port on the device's GUI. A window with that device's port session opens on your desktop.



To switch ports in the viewer, open the hidden Control Panel (by hovering over the top center of the viewerwindow), and select the *Port List* icon. The port list choices include all the ports belonging to the device.

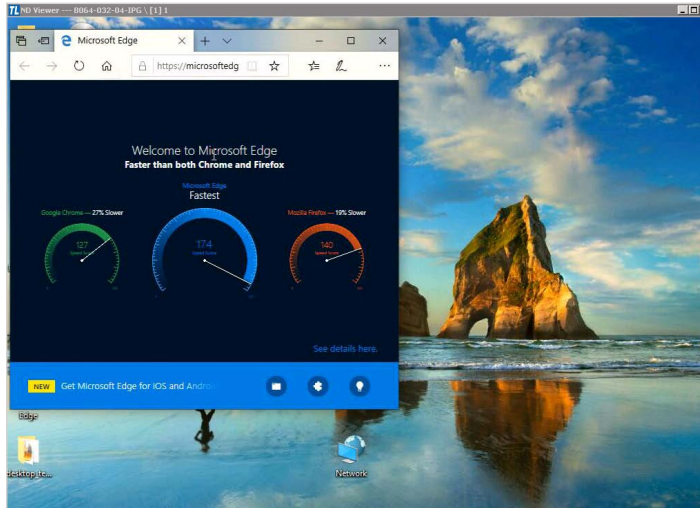


- In the list, select the device the port belongs to (B064-032-04-IPG in the screenshot), then click the port you want to access.
- The device or port name (port ID) displays in the ND Viewer title bar.
- The viewer window of each port has a hidden Control Panel. To switch to a different port on the device, bring up the port list and click the desired port.
- When you have finished with your session, open the Control Panel and select the *Exit* icon.

Note: The ND Viewer does not support OpenJDK.

Web Access

Clicking Web Access opens a browser session for the device on your desktop just as if you had opened your browser and logged into from the URL bar:



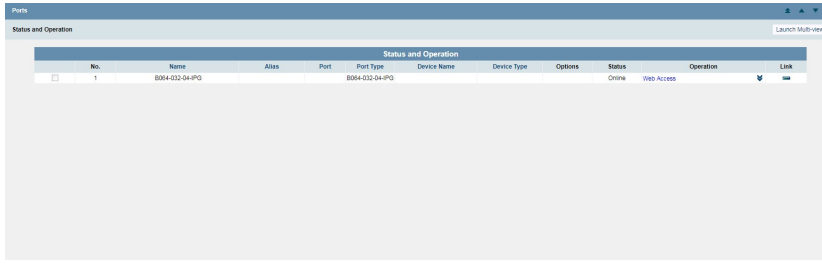
SSH / Telnet Session

Choose to open an SSH or Telnet session to the selected port. You get an SSH or Telnet viewer window just as if you had logged into the serial device (B064-032-04-IPG, for example), with your browser and had chosen *Telnet* on the Main Web page.

Port Access Views

Port View

When Port Access is selected on the tab bar, the default page is Port View. This page lists all of the ports that have been deployed under the NetDirector AXS management system, independently of their devices:



To only see a particular port, click on it in the Sidebar.

Target View

The Target page default view has *All* selected at the top of the Sidebar, and the *Status and Operation* page displayed in the Interactive Display panel:



To only see the ports for a particular device, click on the device in the Sidebar.

Device View

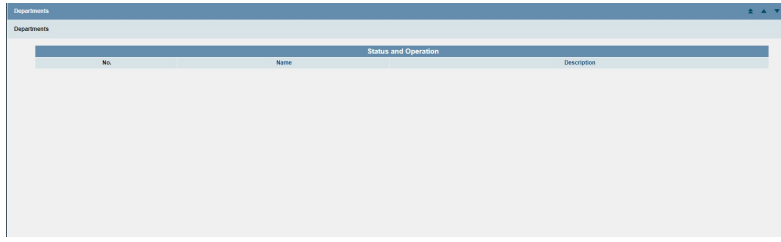
Device view displays all of the devices that have been deployed under the NetDirector AXS management system:



To only see the ports for a particular device, click on the device in the Sidebar.

Department View

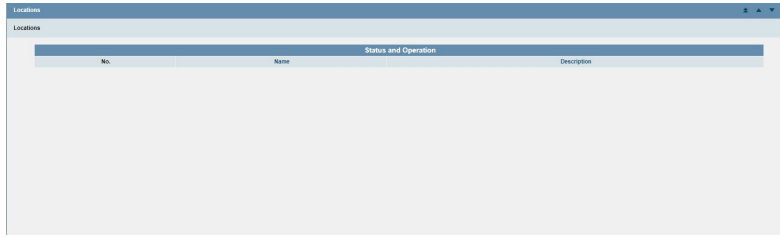
Department view displays all of the departments that have been created under the NetDirector AXS management system, and the ports that have been assigned to each:



To only see the ports belonging to a particular department, click on the department in the Sidebar.

Location View

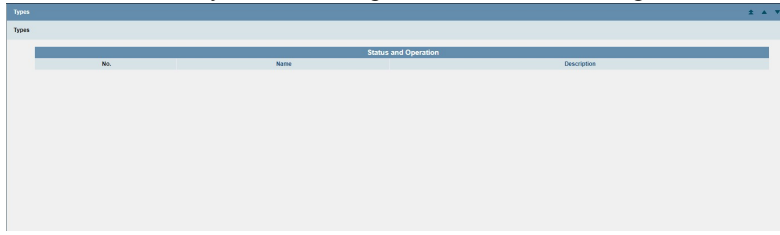
Location View displays all of the locations that have been created under the NetDirector AXS system, and the ports that have been assigned to each:



To only see the ports belonging to a particular location, click on the location in the Sidebar.

Type View

Type View displays all of the device types that have been created under the NetDirector AXS system, and the ports that have been assigned to each:

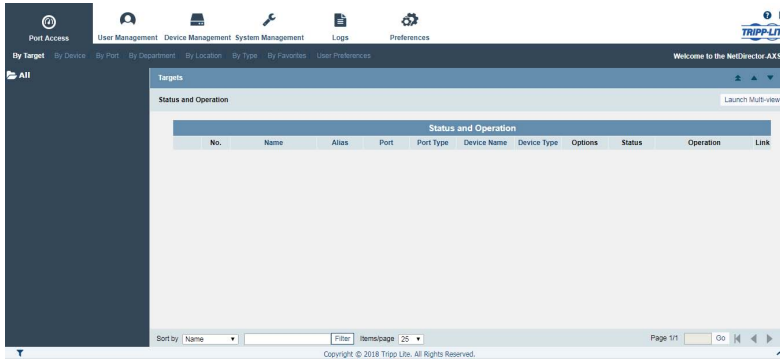


To only see the ports belonging to a particular device type, click on the type in the Sidebar.

Favorites View

The *Favorites* page is similar to a bookmarks feature. Devices and ports that you frequently access can be saved under favorite names of your choosing here. Simply open this page and select the name – rather than hunting for devices and ports in the Sidebar. This feature is especially handy on large, crowded installations.

When you select Favorites on the menu bar, the default page comes up, listing all of the devices and ports that have been deployed under the NetDirector AXS system:

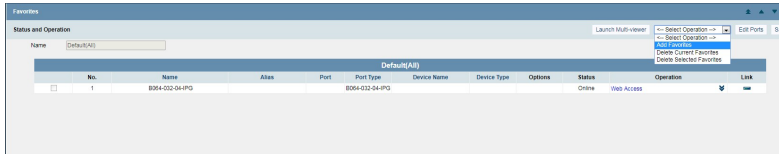


Note: *Filter* and *Launch Multiviewer* work the way they do on the other View pages.

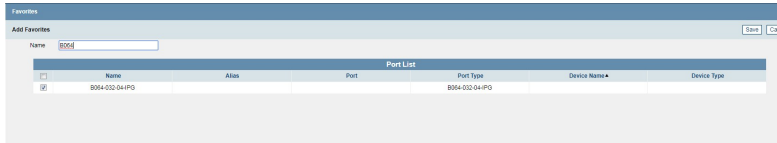
Adding a Favorite

To create a Favorite and populate it with ports, do the following:

1. Drop down the *Select Operation* list and choose **Add Favorites**.



2. In the page that comes up, give the Favorite a name, click the checkboxes of the ports you want to include, then click **Save**.



When the operation completes, your Favorite displays in the main panel, and it is also listed in the Sidebar.

Viewing a Favorite

There is a filter panel at the bottom of the sidebar that lets you control the items that display on this page:



Use of the filter is described in the table, below:

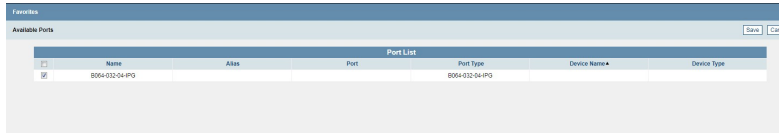
Choices	Explanation
Default	This is the default view. With no other filter options selected, all of the ports that are accessible to the user are listed in the Sidebar and display in the main panel. If any *Favorites* have been created, you can drop down the list box and select the one you want to view. When you select a Favorites, only the items that you have chosen for it display in the Sidebar and main panel.
Online	If you enable *Online* (by putting a check in the checkbox) only the ports whose attached devices are online appear in the Sidebar and the main panel.
Search	If you key in a search string and click **Search**, only port names that match the search string display in the Sidebar and main panel. Partial entries are acceptable, so that key in **Web**, any ports that contain the string *Web* anywhere in their name, show up in the Sidebar and main panel.

Managing Favorites

To add or remove ports from a Favorite. do the following:

1. Select the Favorite in the filter list.
2. Click **Edit Ports** (at the top-right of the panel).

   A page comes up showing all of the ports available to the user, with the ports that are currently included in the Favorite having a check in their checkboxes:



3. Check any ports you want to include in the Favorite; uncheck any ports you want to remove from the Favorite.
4. click **Save**.

User Preferences

The last item on the Menu Bar, *User Preferences*, is different from the other Menu Bar items in that it doesn't provide an organizational view of the devices and ports. It has two Panel Menu items: *Port Display*, and *Alias*. Port Display lets you configure how the device tree appears in the Sidebar; Alias lets you give nicknames to your devices and ports.

Port Display

The Port Display page is the default that opens when you select *User Preferences*.



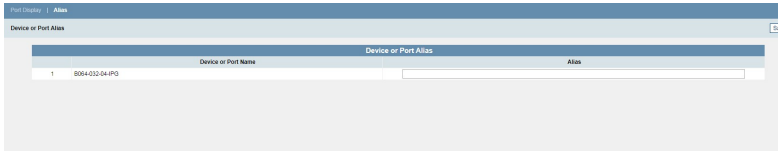
An explanation of the display settings is given in the following table:

Item	Explanation
Display Settings	◆ Drop down the list to select which view you wantthe page to open to when you click the Port Access tab. ◆ If you choose **Show complete tree**, all the nested devices and ports will display when you click to expand the tree. ◆ If you choose **Hide physical devices or ports that are included in group devices**, physical ports that are included in group devices will not display under their originating devices when you click to expand the tree.
View Settings	If you select **Allow group devices to expand in By Device**, ports nested under aggregate or group devices also appear in the tree view. Otherwise, there is no plus sign in front of the group device, and its ports cannot be displayed.

Viewer Client Settings	◆ If you choose **Auto-detect system**, the NetDirector AXS will check to see if you log in with IE or with another browser. If you logged in with IE, it will open the Windows Client Viewer when you access a device or port. If you logged in with a browser other than IE, it will open the Java Client Viewer. ◆ If you choose **Always use java Client**, the NetDirector AXS will open the Java Client Viewer whether which browser you logged in.

Alias

Selecting *Alias* on the Panel Menu, brings up a page that allows you to give your devices, ports, and outlets a nickname to make it more convenient to remember which items you are managing:



- The default view only shows devices. To give an alias to a port or outlet, click the arrowhead in front of the device's name to show them.
- Key the alias into the *Alias* field that corresponds to the device, port, or outlet. When you return to an organizational view page, the alias appears in the Sidebar instead of the device or port name.

Note: The alias only appears for the particular user that creates it. Other users see the original name (or an alias that they have created).

This Page Intentionally Left Blank

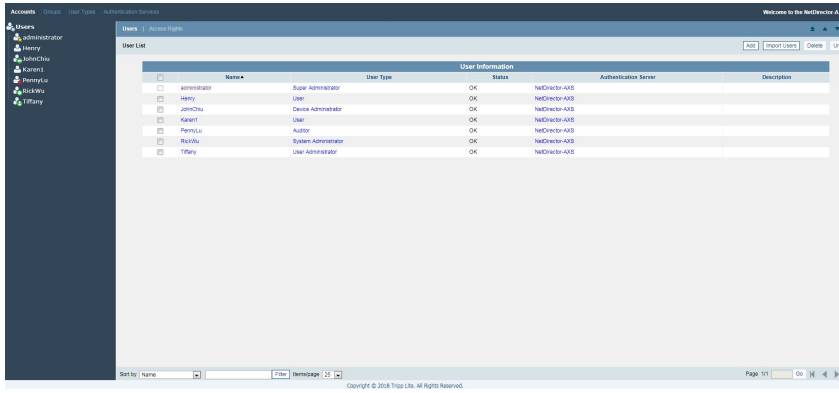
Chapter 5
User Management

Overview

The *User Management* page is used to perform the following functions:

- Add, modify and delete user accounts
- Create user groups and assign users to them
- Specify device access rights for users and groups based on system default or custom defined user types
- Specify whether the user's authentication will be performed via the NetDirector AXS (internal) or via an external authentication server

When you click the User Management tab, the NetDirector AXS opens to the default *Accounts* page, which looks similar to the screen, below:

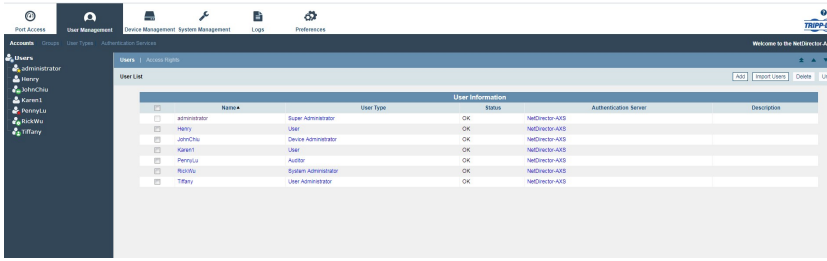


All users and groups, are listed in the Sidebar and in a table in the Interactive Display Panel. To access any user or group, simply click on the name in either location.

Note: The User Management page is for System Administrators and User Administrators. Other user types can omit this chapter.

Accounts

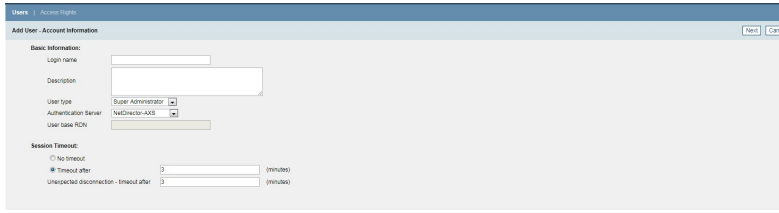
The Accounts page is used to add, modify and delete user accounts. The default Accounts page looks similar to the one below:



Adding User Accounts

To add a user, do the following:

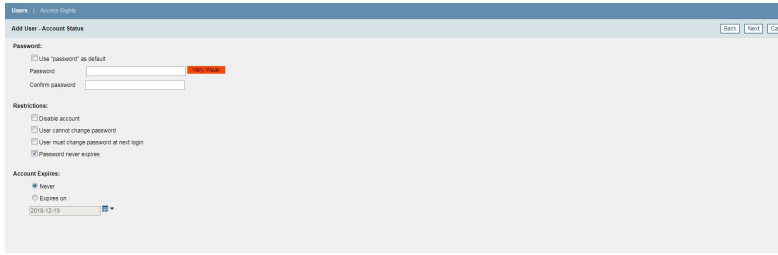
1. Select **Users** in the Sidebar.
2. Click **Add** at the top-right of the main panel. The *Add User - Account Information* page appears:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Login name	**Internal (ND) Accounts:** A maximum of the equivalent of 16 English alphanumeric characters is allowed. The minimum number of characters is based on the NetDirector AXS's account policy settings (see *NetDirector AXS Authentication*, page 72). **External Authentication:** The Login name should be one that exists on the external authentication server. **Note:** These external servers provide authentication services only – they do not provide authorization services. Authorization is provided through the NetDirector AXS management system, hence the access rights need to be set in the NetDirector AXS.
Description	Additional information about the user that you may wish to include. A maximum of 256 Bytes is allowed.
User type	Drop down the list to select the User Type you want to assign the new user to. See p. 69 for information about User Types.
Authentication server	For authentication by the NetDirector AXS, keep the selection as is. For authentication by an external authentication service, drop down the list to select the one you wish to use. **Note:** Before you can make this selection, an external authentication server must first be added. See *External Authentication Servers*, page 73, for details.
User base RDN	If the authentication server is an LDAP server, the user's base RDN setting must be in this field.
Session Timeout	If you don't want to have a session time out after the user has been idle for a specified amount of time, select the *No timeout* radio button. If you do want to have a session time out after the user has been idle for a specified amount of time, select the *Timeout after* radio button. Valid settings are from 1–99 mins. The default is 3 mins. **Note:** This setting pertains to Web log in sessions.
Unexpected disconnection timeout	If the user unexpectedly disconnects (i.e. closes the browser), the NetDirector AXS times out the user's session after the amount of time specified here. The timeout interval is from 3–10 minutes; default is 3 minutes.

4. Click **Next** at the top-right of the main panel. If NetDirector AXS was chosen for authentication, The *Add User - Account Status* page appears:



Note: If an external authentication server was chose for authentication, the account status information is maintained on that server, so this page doesn't appear. Instead, you go directly to the *Add User - Personal Information* page (see step 5).

A description of each of the fields is given in the table below:

Field	Description
Password	◆ Enabling *Use "password" as default* sets **password** as the user's password. ◆ If you do not enable *Use "password" as default*, enter the user's password in the *Password* field. A maximum of the equivalent of 16 English alphanumeric characters is allowed. The minimum number of characters is based on the NetDirector AXS' account policy settings (see *NetDirector AXS Authentication*, page 72). ◆ To be sure there is no mistake in the password, enter it again in the *Confirm Password* field. The two entries must match.

Field	Description
Restrictions	◆ *Disable account* temporarily cancels a user's account without deleting it – so that the account can easily be reinstated at a future time. ◆ If *User cannot change password* is enabled, the user can't change his own password. Otherwise, the user can use the *Preferences* tab to change his own password. See *Password*, page 33 for details. ◆ If *User must change password at next login* is enabled, the user must change his password the next time he logs in. ◆ Enabling *Password never expires*, prevents the user's password from expiring after a given period of time. This overrides the system-wide configuration set on the account policy settings (see *NetDirector AXS Authentication*, page 72). **Note:** Enabling some restrictions automatically disables others.
Account Expires	◆ Clicking the *Never* radio button sets it so that the account never expires. ◆ To have the account expire on a certain date, click the *Expires on* radio button; then click the calendar icon to select the expiration date.

5. Click **Next** at the right of the panel. The *Add User - Personal Information* page appears.

   The fields on this page are optional. You can leave them blank, or fill in as much as you like.

6. When you have finished with the *Add User - Personal Information* page, click **Save** at the top-right of the main panel to bring up the *Add Access Rights* page.

   This page lets you set the user's access rights to the devices and ports that exist on the installation. See *Access Rights*, page 61 for information on the configuration settings.

7. When you have finished setting the user's access rights, click **Save** at the top-right of the main panel to add the user to the *Users* list, and bring up the *Access Rights Summary* page. See *Access Rights*, page 58, for details about adding access rights.

Note: To add additional users, you must start by clicking **Users** in the Sidebar.

Managing User Accounts

To manage a user account do the following:

1. Select **Users** in the Sidebar.
2. Either click the user's name in the Sidebar, or click the user's name in the main panel. The user's Account Information page appears:



This page is similar to the adding a user account page, except there are three Panel Menu items at the top: User Information, Group Membership, and Access Rights.

User Information

This Panel Menu item contains all three pages (Account Information, Account Status, and Personal Information), that were in the Adding a User Account procedure (see page 53). They are used to modify a user's account – such as changing the user's password. To modify the information on these pages, you can either move through them sequentially, by clicking the arrow icons, or you can go directly to a page by hovering over the menu and selecting the page from the popup menu that appears.

Group Membership

Clicking this Panel Menu item brings up a page that shows a list of all the groups a user belongs to. You can click on the group name in the list to go to the group's *Group Information* page. See *Groups*, page 63 for details about this page.

Access Rights

To configure a user's access rights to devices and ports, do the following:

1. Select **Accounts** on the Menu Bar.
2. Select the User in the Sidebar.
3. Select **Access Rights** on the Panel Menu Bar in the Interactive Display Panel to bring up the user's *Access Rights* page.

If no devices have been assigned to theuser, the page that comes up looks like the one shown below:



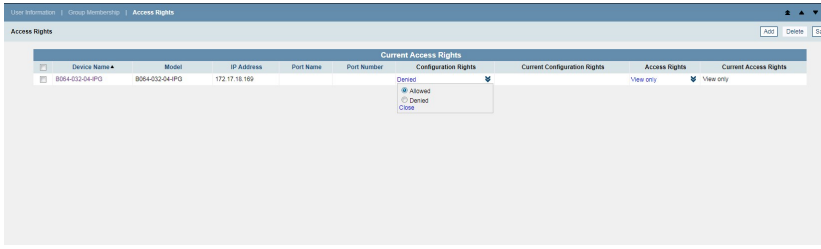
Note: Access rights do not have to be individually assigned in all cases. See *Copy / Paste Access Rights*, page 60, for details.

■ Adding Device Access

To add devices that the user can access, do the following:

1. Click **Add** at the top right of the panel.

   A screen with a list of all the devices on the installation, appears:



2. Check the devices and ports that you want the user to be able to access.

3. For each selected device, port, and outlet, click on the arrow in the *Configuration Rights* column to set the user's configuration rights for that item. **Allowed** means the user can configure the device or port settings; **Denied** means that the user cannot configure the device or port settings.

4. For each selected device, port, and outlet, click on the arrow in the *Access Rights* column to set the user's access rights for that item. An explanation of the access rights is given in the table, below:

Rights	Port Type	Explanation
Full access and VM (Read / Write)	KVM	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse. The user also has read/write rights to use the virtual media function.
Full access and VM (Read Only)		The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse. The user also has read only rights for the virtual media function.
Full access		The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse.
View only		The user can access the device (or specified ports on the device), and view the screen, but cannot perform any operations on it.
No access		The user has no access to the device (or specified ports on the device). The device (or the specified ports) will not show up in the *Port Access* Sidebar or List.
Allowed		The user is allowed to configure the power status of the device (or specified ports on the device).
Denied		The user is not allowed to configure the power status of the device (or specified ports on the device). The device (or the specified ports) will not show up in the *Port Access* Sidebar or List.
Telnet	Serial	The device (or specified ports on the device) must be accessed over a Telnet connection on port 23.
SSH		The device (or specified ports on the device) must be accessed over an SSH connection on port 22.
Administrator		The administrator can perform all configurations and operations.

Rights	Port Type	Explanation
User	Generic; Web Access	The user can perform all operations.
View only		The user can view the screen, but cannot perform any operations.
No access		The user has no access. The Web Access option does not appear as an Operation choice on the Port Access page.

5. When you have finished making your selections, click **Save**.
6. To add access for additional devices, bring up the user's Access Rights page and repeat the procedures described above.

■ **Modifying Device Access**

To change the access rights to a device or port bring up the user's Access Rights page; make the configuration rights and access rights changes to the desired items; then click **Save**.

■ **Removing Device Access**

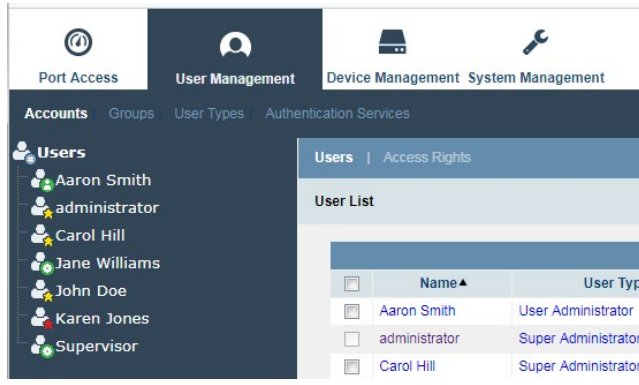
To remove access to a device or port, bring up the user's Access Rights page; click to place a check in the box in front of the device you want to remove; then click **Delete**.

■ **Managing Devices**

You can bring up the Management page of any device, port, or outlet, by clicking on it in the *Device Name* or *Port Name* list.

Copy / Paste Access Rights

The access rights copy-paste function is enabled between compatible nodes (i.e. user to user). To usethis function, in the sidebar tree, right-click on a user's name and select *copy access right*. Right-click on another user and select *paste access right*.



Deleting User Accounts

To delete a user account do the following:

1. Select **Users** in the Sidebar.
2. In the Interactive Display panel, click to put a check in front of the user whose account you wish to delete.



Note: You can delete more than one user by checking as many names as you require. You can delete all deleteable accounts by checking the box at the top of the column.

3. After you have made your selection, click **Delete** at the right of the panel.
4. In the confirmation popup that appears, click **OK**.

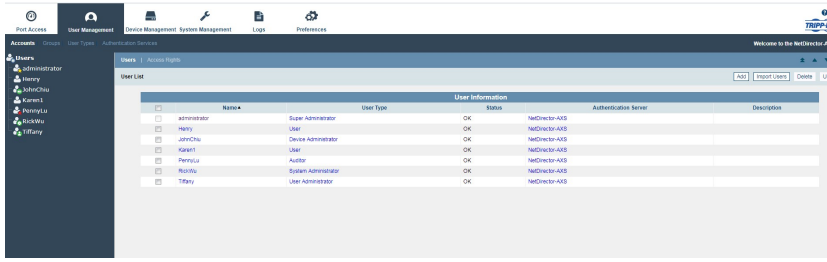
Unlocking User Accounts

If a user has been locked out due to exceeding the number of login attempts, and the *Force manual unlock* option has been enabled (see *Lockout Policy*, page 127), to unlock the user, do the following:

1. Select **Users** in the Sidebar.

   The user account that is locked will show **Locked** in the Status column.

2. In the Interactive Display panel, click to put a check in front of the user whose account you wish to unlock.



3. After you have made your selection, click **Unlock** at the right of the panel.
4. In the confirmation popup that appears, click **OK**.

Note: 1. You can unlock more than one user by checking as many names as you require. You can unlock all locked accounts by checking the box at the top of the column.

2. If all users – including the System Administrator – get locked out, the System Administrator can use the NetDirector AXS Utility to restore his account and unlock the locked out users.

Groups

Groups allow administrators to easily and efficiently manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators need only set them once for the group, instead of having to set them for each user individually. Multiple groups can be defined to allow some users access to specific devices while restricting other users from accessing them.

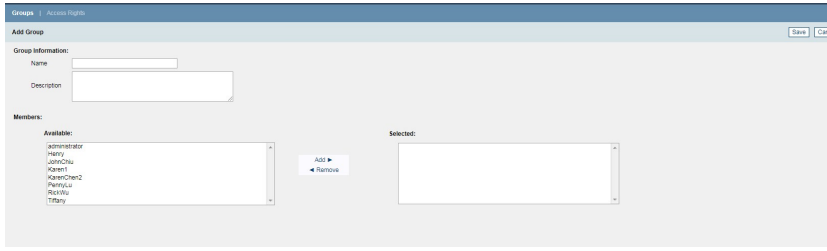
Creating Groups

To add a group, do the following:

1. Select **Groups** from the User Management menu bar. The *Group List* page appears:



2. Click **Add** at the top-right of the main panel. The *Group Information* page appears:



3. Key in a Name and a Description (optional) for the group.

Note: 1. The Name can be the equivalent of from 2–32 English alphanumeric characters, but cannot contain the following: **/ \ [ ] : ; | = , + * ? < > @ " '**

2. The Description can be up to 256 Bytes

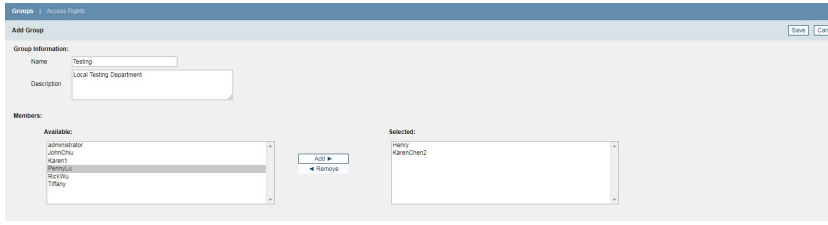
3. Click **Save** to create the group. The group now appears in the Sidebar and the Group Information list in the Interactive Display Panel.

Note: You can add users to the group before performing this step. See the next section for details on adding users to groups.

Adding Users to Groups

To add a user to a group, do the following:

1. Select **Groups** from the User Management menu bar.
2. Either in the Sidebar or the Interactive Display panel, click the group's name. The *Group Information* page appears.



3. Select the user you wish to add to the group from the *Available* list, then click **Add** to move the user from the *Available* list to the *Selected* list.
4. Repeat step 3 for any other users you wish to add to the group.

Note: A shortcut for adding multiple users is to select the ones you want in the Available column using Ctrl+Click or Shift+Click before clicking Add to move all the selected ones at once.

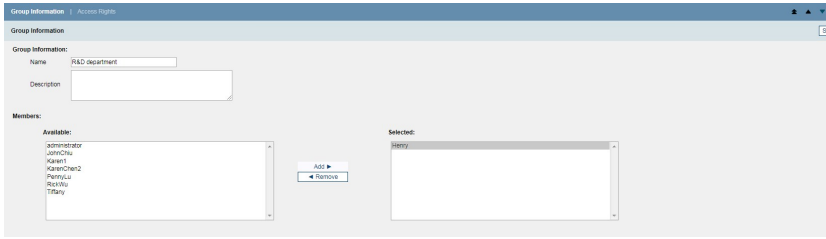
5. When you have finished adding users, click **Save** to complete the procedure.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users from Groups

To remove a user from a group, do the following:

1. Select **Groups** from the User Management menu bar.
2. Either in the Sidebar or the Interactive Display panel, click the group's name. The *Group Information* page appears.



3. Select the user you wish to remove from the group from the *Selected* list, then click **Remove** to move the user from the *Selected* list to the *Available* list.
4. Repeat step 3 for any other users you wish to remove from the group.

> **Note:** A shortcut for removing multiple users is to select the ones you want in the Selected column using Ctrl+Click or Shift+Click before clicking Remove to move all the selected ones at once.

5. When you have finished removing users, click **Save** to complete the procedure.

Access Rights

To configure the access rights for a group, do the following:

1. Select **Groups** from the User Management menu bar. The *Group List* page appears.
2. Select the group that you want to configure the access rights for.
3. In the *Group Information* page that comes up, select **Access Rights** on the Panel Menu bar:



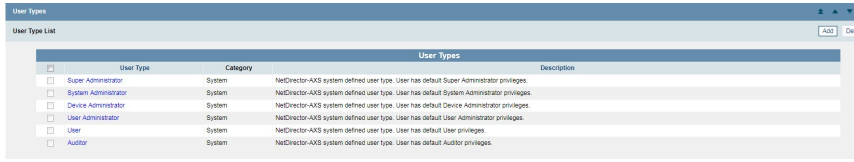
The procedures for configuring Group access rights are similar to the ones described for User Accounts.

User Types

There are two major categories of user types: System and Custom. By default, the NetDirector AXS supports six user types. These are referred to as *System* user types because they are built in to the system. The roles assigned to members of these user types are fixed and cannot be changed.

The *Custom* user type category, by contrast provides you with the convenience and flexibility of assigning various combinations of roles that best suit your installation's requirements.

When you click **User Types** on the menu bar, the *User Type List* appears in the Interactive Display panel, showing all the user types that have been configured:



Members

Clicking a user type in the Sidebar or in the Interactive Display panel brings up the *Members* Panel Menu page showing all the users that belong to that type.



- Clicking a user's name brings you to that user's *Account Information* page.
- To add a user to the type, click **Add** at the top-right of the main panel. In the page that comes up, select the user you would like to add, then click **OK**.
- To change the user's type, check the box in front of the user's name, then click **Change** at the top-right of the main panel. In the page that comes up, select the new type for the user, then click **OK**.

Type Information

When you are in the *Members* page, you can click **Type Information** to see a description of that user type, as well as, the roles that are assigned to it:



Note: The only change you can make on this page is in the *Description* field where you can provide additional information about the user type.

System Types

The roles performed by members of the System category are fixed. The roles associated with each type are summarized in the table below:

Assigned Roles	Super Admin	System Admin	User Admin	Device Admin	User	Auditor
System configuration and settings	√	√				◊
# # # #	#					
	√	√				◊
System tasks	√	√				◊
#	√	√				◊
Authentication services	√	√	√			◊
User / Group management	√	√	√			◊
User / Group device access rights	√	√	√			◊
Device management	√	√		√		◊
Log configuration and setting	√	√	√	√		
View logs	√	√	√	√		◊
Users can change their own passwords	√	√	√	√	√	√

Note: 1. The differences between the Super Administrator and The System Administrator are as follows:

- The Super Administrator is authorized for all roles automatically, and includes access to all devices and ports. The roles are fixed and can't be changed.
- Each of the System Administrator's roles can be assigned manually, and access to devices and ports must be assigned manually.
- The Super Administrator's user type can't be changed; the System Administrator's type can be changed.

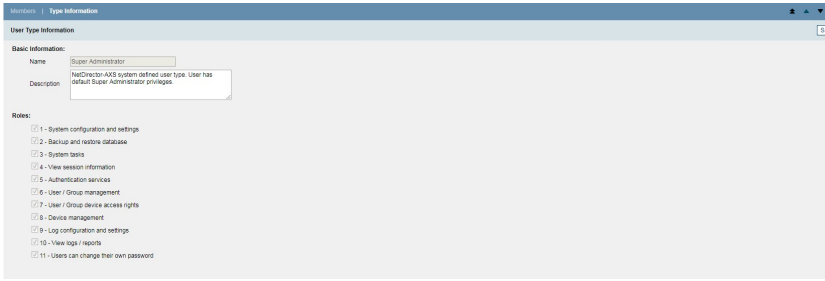
2. With regard to the *Auditor* type:

- The Auditor type can access all tabs and pages, but is restricted to *View Only* rights.
- Under the **Log** tab, the Auditor type can export and print logs in addition to viewing them, but cannot change any settings.
- Under the **Preferences** tab, the Auditor type can change his/her *Color Scheme*, *Web Options*, and *Password* settings.

Custom Types

The NetDirector AXS provides the ability to create custom user types, with any combination of roles assigned to them, which may better suit your requirements than the pre-defined System types. To create a custom user type, do the following:

1. Select **Types** from the User Management menu bar.
2. In the Sidebar, click **Custom Types**. The *User Type List* appears, showing all the Custom user types that have been configured.
3. Click **Add** at the top-right of the panel. In the page that comes up, key in a name and description for the new type, then check the roles you want the new user type to perform.



Note: 1. The Name can be the equivalent of from 2–32 English alphanumeric characters, but cannot contain the following: **" ' **

2. The Description can be up to 256 Bytes.
3. Some roles may appear gray (and are unselectable) due to theuser role restriction policy. See *User Role Restriction Policy*, page 162.

4. When your selections have been made click **Save**.

Authentication Services

The NetDirector AXS provides an internal *Username / Password* authentication service. In addition, the NetDirector AXS supports the following third party external authentication servers: LDAP, LDAPS, Active Directory, RADIUS, TACACS+ and Windows NT Domain.

Note: 1. *Authentication* refers to determining the authenticity of the person logging in; *authorization* refers to assigning permission to use the device's various functions.

2. These external servers provide authentication services only – they do not provide authorization services. Authorization is provided through the NetDirector AXS system.

By adding an external authentication server to the NetDirector AXS system (see page 73 for details), when you add a user account, you can select the external authentication server from the list of authentication servers (see *Adding User Accounts*, page 53).

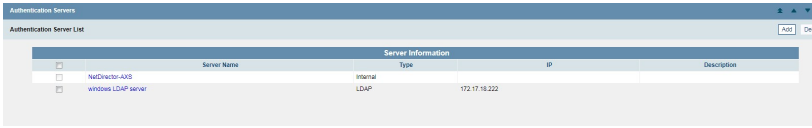
Note: For LDAP, LDAPS, and Active Directory there is an additional authentication method in which the user attempting to log in does not have an account on the NetDirector AXS. In this case, the NetDirector AXS checks the external server to see if it contains an account with the username and password of the user attempting to log in. If it does, the NetDirector AXS checks to see if the user belongs to a group that corresponds to a group that exists on the NetDirector AXS. If it does, the NetDirector AXS lets the user log in and assigns him the access rights of the group. See *Group Authorization*, page 77, for details

---

(Continues on next page.)

(Continued from previous page.)

When you click **Authentication Services** on the menu bar, the *Authentication Server List* appears in the Interactive Display panel, showing all the authentication services that have been configured:



NetDirector AXS Authentication

With regard to the NetDirector AXS' internal authentication services, there are some configuration settings you can make to the password policy function. All user accounts must follow the requirements you set here. To configure the NetDirector AXS' password policy, do the following:

1. Select **Authentication Services** from the User Management menu bar.
2. Either in the Sidebar or in the Interactive Display Panel, click ND.

   The *Properties* page appears



3. Make the configuration choices you desire. (Refer to the table, below, for an explanation of the fields.)

Minimum username length	The username length can be the equivalent of from 1–16 English alphanumeric characters. The default is 6 characters.
Minimum password length	The password length can be the equivalent of from 0–16 English alphanumeric characters. The default is 6 characters. A setting of 0 means that no password is required. Since this leaves your installation in a highly insecure state, we strongly recommend against a setting of 0.
Password expiration	For security purposes you can force users to renew their passwords at specific time intervals. To do so, enable *Password expiration*, then specify the number of days that the password will expire after. Once a password expires, a new one must be set. Passwords start expiring from the time an account is created, or a new password is set.
Passwords must contain both letters and numbers	For security purposes, enable this setting to force the user to include both letters and numbers in the password.
Passwords must contain both upper and lower case letters	For security purposes, enable this setting to force the user to include both upper and lower case letters in the password.

4. When you have finished, click **Save**.

External Authentication Servers

Adding an External Authentication Server

In order to use a third party external authentication server, you must first add it to the Authentication Server list. To do so:

1. Select **Authentication Services** from the User Management menu bar to bring up the Authentication Server list:



2. Click **Add** at the top-right of the main panel. In the *Add Authentication Service* page that appears, drop down the Server type list to select the service you want to add; give it a name and description, then click **Next** at the top-right of the panel.



3. The page that comes up next depends on the service you have chosen. Follow along with the Wizard's pages, keying in the information required for the external authentication server you selected. When you have finished, click **Save**.

Note: 1. The Server name can be the equivalent of from 2–32 English alphanumeric characters, but cannot contain the following: **" '**

2. The Description can be up to 256 bytes.

Service Information

An explanation of the information required for each of the services is provided, below.

1. LDAP/LDAPS

Heading	Information
Connection Settings	Get the information for these fields from the LDAP administrator. The port default is 636, but check with the LDAP/LDAPS administrator to see if it may be something else.
SSL Mode	◆ Click the *Do not use SSL* radio button to use LDAP. ◆ Click the *Use SSL in Trust All mode* radio button to use LDAPS.
LDAP User Schema	Get the information for these fields from the LDAP administrator.
Browsing Method	When adding or modifying user accounts (see *Adding User Accounts*, page 53), you can click the **Browse** button to browse all users in *User RDN* to choose the Login name. ◆ Select *Browse with user credentials* to allow the user to browse LDAP/LDAPS using credentials configured on the server. If this is selected the user doesn't have to input his credentials each time he browses. ◆ Select *User must input credentials when browsing* to have the user input his credentials each time he browses the LDAP/LDAPS.

2. Active Directory

Heading	Information
Connection Settings	Get the information for these fields from the Active Directory administrator.
SSL Mode	Click a radio button to choose whether or not to use SSL in Trust All mode.
Browsing Method	◆ Select *Browse with user credentials* to allow the user to browse the Active Directory using credentials configured on the server. If this is selected the user doesn't have to input his credentials each time he browses. ◆ Select *User must input credentials when browsing* to have the user input his credentials each time he browses the Active Directory.

3. RADIUS and TACACS+

Heading	Information
Connection Settings	Get the information for these fields from the service administrator. The default for RADIUS is 1812; the default for TACACS+ is 49, but check with the service administrator to see if it may be something else.
Authentication Settings	Get the information for these fields from the service administrator. 1. Drop down the list to select the *Authentication type* your RADIUS server is configured for. 2. In the Shared Secret field, key in the character string that you use for authentication with the RADIUS server. 3. Key the shared secret in again in the Confirm Shared Secret field.

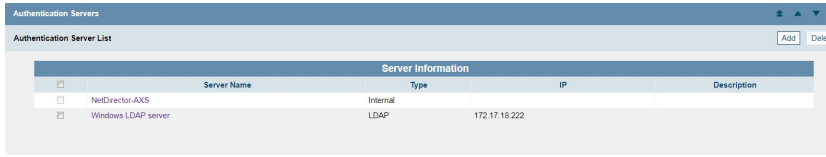
4. Windows NT Domain

   Get the information for the Domain Name from the service administrator.

Deleting an External Authentication Server

To delete an external authentication server, do the following:

1. Select **Authentication Services** from the User Management menu bar to bring up the Authentication Server list:
2. In the Interactive Display panel, click to put a check in front of the external authentication server you wish to delete.



Note: 1. You can delete more than one server by checking as many names as you require.

2. You can delete all deleteable servers by checking the box at the top of the column.
3. If a user account has been created on the NetDirector AXS that uses an external authentication server, the server can't be deleted.

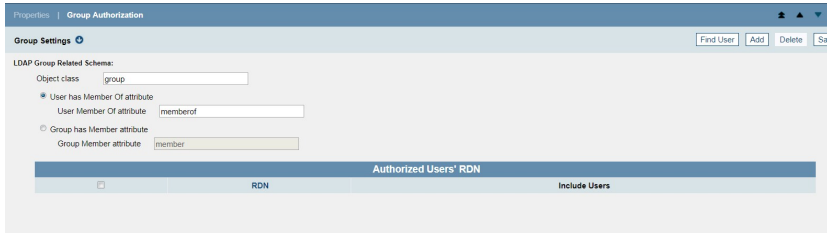
3. After you have made your selection, click **Delete** at the right of the panel.
4. In the confirmation popup that appears, click **OK**.

Group Authorization

For LDAP, LDAPS, and Active Directory there is an additional authentication method in which the access rights for a specified group are set. This function is used to make it easier to authorize users with accounts on an external authentication server. Instead of having to authorize the user on a rights-by-rights basis, the administrator assigns the user to a group, and the user inherits the rights that the group has.

To add a group for group authorization, do the following:

1. Under *User Management* → *Authentication Services*, select the external authentication server from the Sidebar or the main panel list. The server's *Properties* page comes up.
2. Select **Group Authorization** (on the Panel Menu bar). The *Group Authorization* page appears:



Note: 1. The screenshot shows a page that appears if an LDAP service was chosen. The LDAP Group Related Schema settings fields do not appear if Active Directory was selected.

2. For the LDAP Group Related Schema settings, get the information for these fields from the LDAP administrator.
3. The default setting for OpenLDAP is *Group has Member attribute.*

   The alternative setting is *User has Member Of attribute.*

4. There are two methods to add users to an authorization group:
   - Click **Add**. In the page that comes up either key in the user's RDN, or retrieve it with the *Browse* button, then click **Save**.

     – or –

   - Click **Find User** to see a list of all users in the server's database, then select the user from the list.
5. In the *Properties* page that comes up, key in the *Basic Information* and *Session Timeout* information.

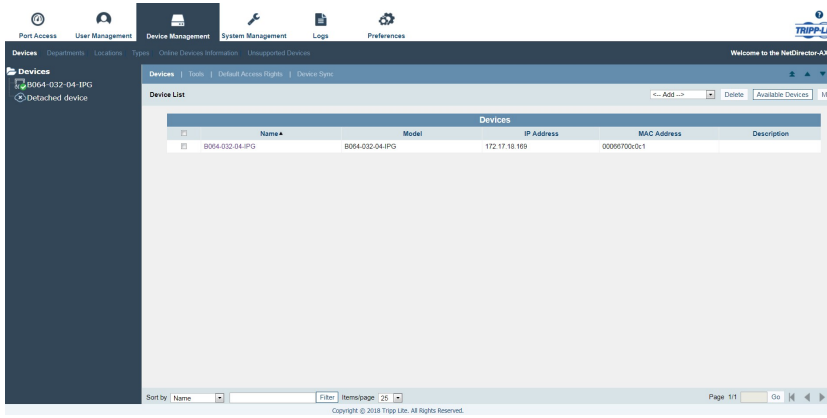
   Note: This page is similar to the adding user account page, see *Adding User Accounts*, page 53 for settings details.

6. In the Sidebar, or the main panel, select the group you just added.
7. Select **Access Rights** on the Panel Menu bar, then click **Add**. A list of available devices appears. See *Access Rights*, page 58 for information on how to assign access rights on this page.
8. After you have made your access rights selections, click **Save** (at the top-right of the panel).

Chapter 6
Device Management

Overview

The *Device Management* page is used to add, configure, and organize the devices that will be managed over the NetDirector AXS network. When you click the Device Management tab, the NetDirector AXS opens to the default *Devices* page, which looks similar to the screen, below:



All devices and device folders that have been configured for use on the NetDirector AXS server and have been added into its database are listed in the Sidebar and in a table in the Interactive Display Panel. To access any device item, simply click on it in either location.

Note: The Device Management page is for System Administrators and Device Administrators. Other user types can omit this chapter.

Preliminary Procedures

Before devices can be managed, they must first be added into the system. This involves four basic steps:

1. Connecting the devices to the same network segment as the NetDirector AXS.
2. Once the devices have been connected to the same network segment as the NetDirector AXS, the NetDirector AXS managing that segment must be made aware of them. This can be done either by enabling the *ND Management* function on the device's ANMS page, or with the *Initialize devices IP/Port* function on the *Tools* menu (see page 101).

Note: 1. Secondaries can make sure that the devices that are connected to them have been successfully recognized by clicking the *Show Available Devices* button (at the top-right of the panel).

2. Clicking the server's *Show Available Devices* button lists all the available devices.
(This gives the same result as dropping down its **Add** device list.)
3. Devices that already have been added to the NetDirector AXS management system do not show in the list of available devices.

3. Next, from the NetDirector AXS unit, the devices recognized in step 2 must be added to the NetDirector AXS' management system.
4. Finally, devices can be created either as actual physical port devices (by unlocking each port), or by combining various ports into logical device constructs (Aggregate Devices, Group Devices, etc.). See *Adding an Aggregate Device*, page 90, for details.

Using VPN

In some installations you may prefer to use a VPN (virtual private network) environment for your NetDirector AXS management functions. In this configuration, it is not necessary for the device to be recognized by the NetDirector AXS that manages its network segment. It can be recognized directly by the NetDirector AXS server. This is accomplished by enabling the ND Management functionand keying in the IP address of the NetDirector AXS server you want the device to be recognized by. See *VPNs*, page 165, for more details.

Menu Structure

The Device Management menu structure is described in the table below:

Tab	Page Menu	Panel Menu	Page
Device Management	Devices	Devices	82
		Tools	101
		Default Access Rights	103
		Device Sync	104
	Sidebar Device Tree	Properties (KVM)	105
		Access Rights (KVM)	108
		Device Configuration (KVM)	112
		Port Configuration (KVM)	113
	Departments, Locations, Types		115
	Unsupported Devices		118

Devices

The Devices menu has three Panel Menu items: Devices, Tools, and Device Sync. Its default page is the main page of the Devices Panel Menu. The *Devices* Panel Menu is discussed in the following section; the *Tools* Panel Menu is discussed on page 101; the *Device Sync* Panel Menu is discussed on page 104.

Devices

The Devices Panel Menu is used to add, modify, delete, and organize devices and device folders. All device items that have been configured for use on the ND server and have been added into its database are listed in the Sidebar.

On NetDirector AXS server, device types that can be added and configured are found under the *Add* drop down list at the top of the main panel.

The device types, and an explanation of their purposes are given in the following table:

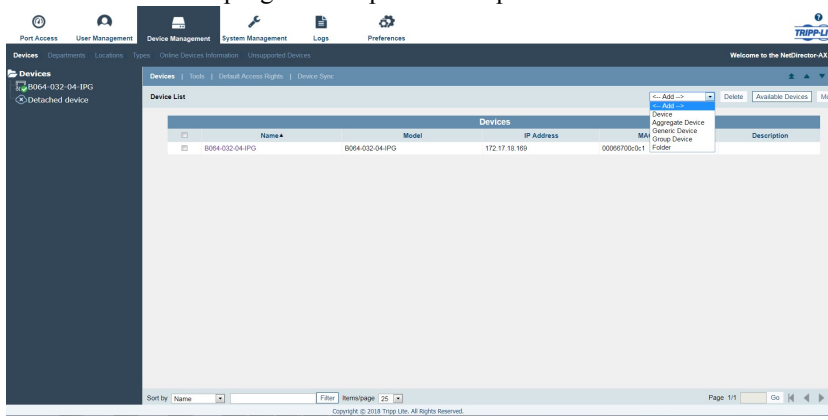
Type	Purpose
Device	Select this type to add Tripp Lite over IP KVM devices into the NetDirector AXS system. NetDirector AXS supports B064 series devices. **Note:** When devices are added all of their ports are locked by default and must be unlocked. See *Locking / Unlocking Ports*, page 99, for details.
Generic Device	Third party generic devices (routers, switches, etc.) can consist of any device that contains an Ethernet interface and can be accessed by its URL or IP Address via HTTP/HTTPS, or Telnet/SSH.Since these devices have no provision for ND management, they cannot be authenticated through the NetDirector AXS, and are not part of the NetDirector AXS' single sign on configuration. There is no proxy support support for these devices When you select this type of device the NetDirector AXS redirects to the device, itself. You must log in to the device using its own authentication procedure.

Type	Purpose
Group Device	Group devices are also created as a composite of ports that exist on actual Tripp Lite over KVM devices. The differences between Group and Aggregate Devices are as follows: Once a physical port is added to an Aggregate device, it cannot be used with any other Aggregate Device – whereas a physical port can be added to any number of Group Devices
Folder	Device folders provide another method (in addition to Departments and Locations) of organizing related devices into useful categories. (Putting all B064 series into one folder, for example.) Doing so makes it easy to configure and maintain similar types of objects. **Note:** 1. Folders are containers for devices, and as such do not count against the number of licensed nodes. 2. Since Folders are organizational tools for device management, they do not show up in the Port Access Sidebar or main panel list.

Adding a Folder or Device

To add a folder or device, do the following:

1. Click *Add* at the top right of the panel to drop down the list of items that



> **Note:** Before dropping down the list, you can click **Show Available Devices** for a list of the physical devices that are available.

2. Click on the item in the list that you would like to add. Depending on your selection, a page appears to provide the interface to set it up.

The sections that follow describe the procedures involved for setting up each of the devices listed.

■ Adding Folders

Creating folders is an organizational option (in addition to *Departments* and *Locations*) that allows you to organize your enterprise-wide devices into useful categories. When you select *Folder* as an item to be added, the *Add Folder* page comes up:



Fill in a name (B064-032-04-IPG-All, for example), and a description (optional) for the folder, then click **Save**. The new folder is added to the Sidebar and the Device List table.

To place devices inside a folder, first select the folder in the Sidebar, then go through one of the *Add* procedures, described below.

Note: 1. The only way that devices can be placed inside of folders is to add them after the folder you want to place them in has been selected.

2. Folders can be nested. Simply go through the adding a folder procedure after selecting the parent folder in the Sidebar.

■ Adding Devices

This item refers to adding Tripp Lite over IP KVM devices into the NetDirector AXS system. NetDirector AXS supports B064 series devices.

Note: 1. Before attempting to add an Tripp Lite over IP KVM device to the NetDirector AXS server, make sure it has been recognized. See *Preliminary Procedures*, page 80, for details.

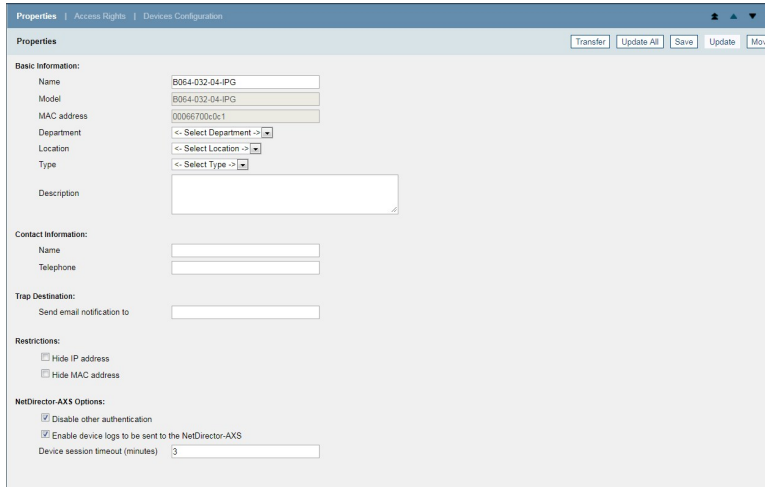
2. If you want to see a list of devices that are available to be added, click **Show Available Devices** (at the top-right of the panel)

When you select *Device* as an item tobe added, the *Choose Device* page comes up listing all the online devices that can be added:



To add a device, do the following:

1. Click to put a check in the checkbox in front of the device you wish to add.
2. Click **Next**. The *Properties* page come up:

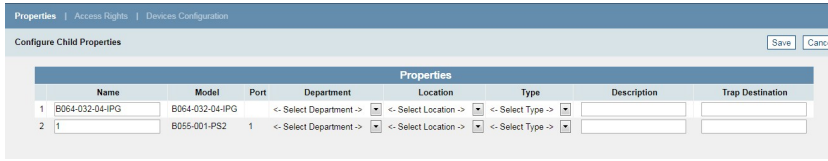


3. Fill in the fields according to the information provided in the table, below:

Field	Information
Basic Information	**Name:** Provide a name to identify the device. The default is the name given to the device under its independent configuration. If you change the name here, the change only takes place in the NetDirector AXS database. The name on the original configuration remains the same. **Model:** The NetDirector AXS recognizes the device model and fills in this field automatically. It cannot be edited. If the device is a Cat5e KVM switch, the KVM Adapter Cable model displays here. **MAC Address:** The NetDirector AXS fills in this field automatically. It cannot be edited. **Department:** For organizational purposes you can establish department categories (R&D, for example), and assign devices to them. If you wish to assign this device to a department, drop down the list of departments (you have previously created – see *Departments, Locations and Types*, page 115), and click on the one you want the device to belong to. **Location:** For organizational purposes you can establish location categories (West Coast, for example), and assign devices to them. If you wish to assign this device to a location, drop down the list of locations (you have previously created – see *Departments, Locations and Types*, page 115), and click on the one you want the device to belong to. **Type:** For organizational purposes you can specify the type of device that this is. If you wish to do so, drop down the list of types (you have previously created – see *Departments, Locations and Types*, page 115), and click on the one you want. **Description:** If you wish to provide extra information to describe the device, enter it here. This field is optional.
Contact Information	The name and telephone number of the device administrator. These fields are optional.
Restrictions	**Hide IP Address:** As an added security measure, if this feature is enabled, it keeps the device's IP address from appearing in the Port Access *Status and Operation* List when users log in via their browser. **Hide MAC Address:** As an added security measure, if this feature is enabled, it keeps the device's MAC address from appearing in the Port Access *Status and Operation* List when users log in via their browser.

Field	Information
NetDirector Option	**Disable other authentication:** As an added security measure, if this feature is enabled, the device will only accept logins through the NetDirector AXS. While the device is connected to the NetDirector AXS system, users cannot log in to the device using the device's own authentication system, and they can only manage the device through the NetDirector AXS' interface. **Note:** 1. If the device becomes disconnected from the NetDirector AXS system, users will be able to log into the device using its own authentication system. 2. If the checkbox is unchecked it means that other authentication is enabled and users can log into the device using its own authentication system. **Enable device log information to be sent to the NetDirector AXS:** If this feature is enabled, the NetDirector AXS acts as the device's log server – receiving and storing the device's tick event information, and having it available for retrieval. **Enable monitor data to be sent to the NetDirector AXS.** If this feature is enabled, environment data that is being monitored is sent to the NetDirector AXS to be recorded in its log files. After enabling this feature, drop down the list to set the **Time interval** between transmissions. **Device session timeout:** If this feature is enabled If there is no input from the user for the amount of time set with this function, the session is terminated. The setting range is 2–99 minutes. A setting of 0 (zero) disables this function. The default is 3 minutes.

4. When you have finished, click **Save** to complete the procedure. You go to the *Configure Child Properties* page, where you can configure properties, as shown below:



5. When you have finished filling in the fields, click **Save**. The *Access Rights Summary* page comes up:



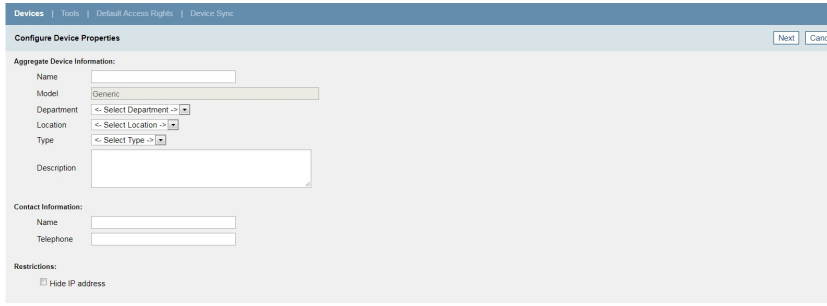
6. Drop down the list to select the user or group you want to set the access rights for.
7. Click the arrow in the Access Rights column; check the appropriate boxes; then click **Save**.
8. Repeat steps 6 and 7 for any additional users and/or groups.
9. Click **Save** to complete the procedure.

Note: 1. After adding a device, its ports are locked. See *Locking / Unlocking Devices*, page 99, for details.

2. For Cat5 KVM switches, only the ports that are have a KVM adapter cable attached, and are online are recognized and are added to the Device List. This is because each adapter cable has its own independent identity and if it is not online there is no way for it to be recognized. Once a port has been added, it will appear in the list even if it is off line.

■ Adding an Aggregate Device

When you select *Aggregate Device* as an item to be added, the *Add Aggregate Device* page comes up:

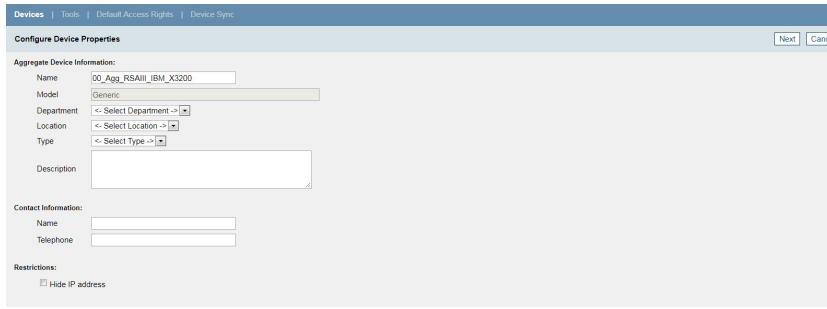


To add an Aggregate Device, do the following:

1. Select the Aggregate Device Model from the drop-down menu. Then, Fill in the fields according to the information provided in the table, below:

Field	Information
Auto Detect	If you are adding one of the specifically mentioned Aggregate Device Model types and enable Auto detect, the NetDirector AXS will check if the device is online. Only a user with administrator privileges can enable this function.
Detect Interval	Set the detect interval by entering a value in seconds. This is how often the system automatically checks that the Aggregate Device is online.
IP	Key in the Aggregate Device's IP address Click **Test Connection** to confirm that the IP has been correctly detected.
Connect Method	Select either SSH or Telnet from the drop-down menu.
Port	Key in the access port used to connect to it (via browser). The default SSH port is 22; Telnet is 23.
Username / Password	Key in a username and password that will be required to access the Aggregate Device.
Login name field / password field	Key in the information so the NetDirector AXS knows where to put the login name and password information under certain single sign-on situations
Timeout	The amount of time to wait for a connection request to complete before canceling the request.
Server	Select the NetDirector AXS unit that the Aggregate Device server is connected under.

2. In the *Configure Device Properties* page, provide a name to identify the aggregate device in the *Name* field.



3. (Optional) Provide a further description of the aggregate device in the *Description* field.
4. (Optional) Drop down the Department, Location, and/or Type list(s) and click on the one(s) you want the aggregate device to belong to.
5. (Optional) Provide the name and telephone number of the device administrator in the *Contact Information* field.
6. (Optional) Set the Power Control Options as outlined, below:
   - Click the box to enable confirmation for power operation
   - Click the box to enable delay for power operation, and set the Power on delay/ Power off delay fields in seconds.

Note: If the SPMs does not support this function, option will not work.

7. When you have finished with this page, click **Next**. The *Configure Network Connectivity* page comes up:



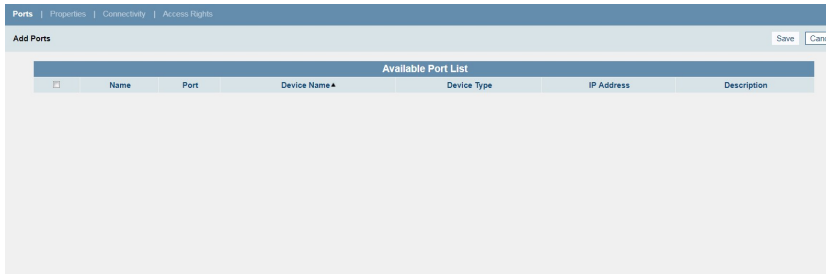
8. Fill in the fields according to the information in the table, below:

Field	Explanation
Network Information	**Select network:** If the server for the aggregate device only has one network interface, then move on to configure the remaining fields. If it has more than one network interface, after you finish configuring the NetDirector AXS server, come back to choose the additional ones and configure each of them in turn. **Name:** For convenience, each of the network interfaces can be named. **IP Address:** Enter the Aggregate Device's IP address here. **Access Type:** Drop down the list to select the access type. Only the *Generic* option supports VNC and RDP connectivity. **Server:** Select the NetDirector AXS unit that the Aggregate Device server is connected under.
Web Session	**URL:** To access the Aggregate Device server via the Web, key in the URL that will bring up its management page. **Enable SSO**: Check this box to enable single sign on functionality, and then select which credentials to use. ◆ Select *Use login user credentials* to use the same account username and password as the NetDirector AXS user account. ◆ Select *Use following credentials* and enter new credentials in the fields below. **Login name, Password:** Fill in these fields according to the Aggregate Device server's authentication and authorization procedures. **Note:** Due to frequent updates applied to browsers, JRE, and SPM firmware, some compatibility problems may occur that affect support for SPM and SSO with the NetDirector AXS.
Login name field / password field	Key in the information so the NetDirector knows where to put the login name and password information under certain single sign-on situations
SSH/Telnet Session	**IP address, Login name, Password, SSH / Telnet port:** To access the Aggregate Device server via an SSH / Telnet session, key the appropriate information into these fields according to the Aggregate Device server's authentication and authorization procedures. **Note:** An SSH session also requires entering login string information
VNC Session	**Port:** Enter the port number for the VNC session **Enable SSO**: Check this box to enable single sign on functionality, and then enter *View only* and *Full control* passwords.
RDP Session	**RDP Port:** Enter the port number for the VNC session **Enable SSO**: Check this box to enable single sign on functionality, and then select which credentials to use. ◆ Select *Use login user credentials* to use the same account username and password as the NetDirector AXS user account. ◆ Select *Use following credentials* and enter new credentials in the fields below.

■ Adding Ports to an Aggregate Device

To add ports to your Aggregate Device, do the following:

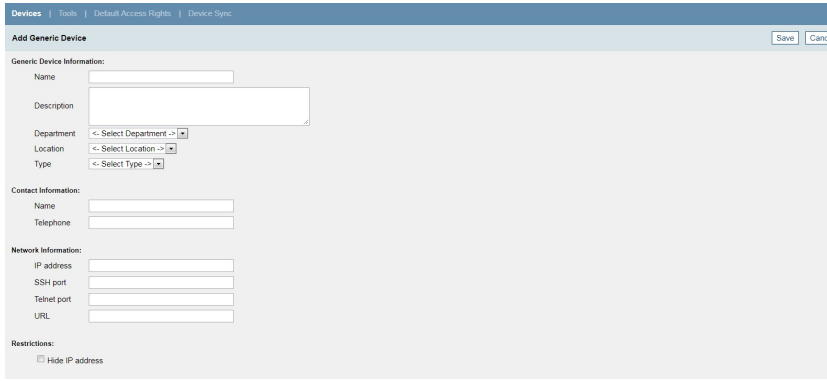
1. Select your Aggregate Device in the Device List or the Sidebar. The *Port List* page comes up.
2. Click **Add** (at the top-right of the panel). The *Add Ports* page appears, listing all available ports that can be added:



3. You can combine any of the ports that are listed on the page in the Aggregate Device. Put a check in the checkbox in front of the ports that you want, then click **Save**.
4. If a port is already part of another aggregate or group device, a dialog box appears to notify you that it will be removed from the original device when added to this aggregate device and asks you to confirm that this is what you want to do. Click **OK** to accept the change or Cancel to abort.
5. When you return to the *Port List* page. The selected ports are automatically unlocked and are listed as being associated with the Aggregate Device. The ports are also nested under the Aggregate Device in the Sidebar.

■ Adding a Generic Device

When you select *Generic Device* as an item to be added, the *Add Generic Device* page comes up:



Note: See *Generic Device*, page 82, for an explanation of generic devices.

1. Fill in the fields according to the information provided in the table, below:

Field	Information
Device Information	**Name:** Provide a name to identify the device. **Description:** If you wish to provide extra information to describe the device, enter it here. This field is optional. **Department:** For organizational purposes you can establish department categories (R&D, for example), and assign devices to them (see *Departments, Locations and Types*, page 115). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes you can establish location categories (West Coast, for example), and assign devices to them (see *Departments, Locations and Types*, page 115). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Drop down the list to select the type of device it is.

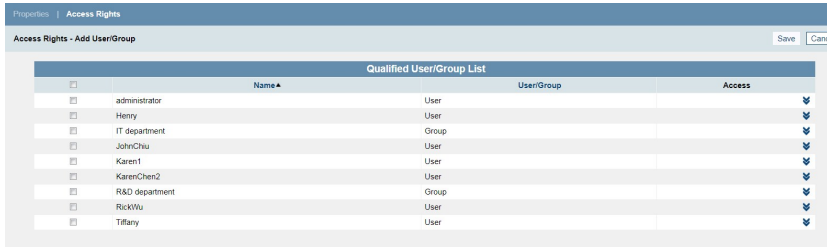
Field	Information
Contact Information	The name and telephone number of the device administrator. These fields are optional.
Network Information	Fill in the fields according to the following information: ◆ If the Generic Device is to be accessed via a web browser, key its web (or IP) address in the URL field. ◆ If the Generic Device is to be accessed via Telnet or SSH, key in the IP Address in the IP Address field and the Telnet and/or SSH port numbers in their corresponding fields. ◆ If the Generic Device has all three methods available, you can fill in all or any of them that you wish.
Restrictions	As an added security measure, if *Hide IP Address* is enabled, the device's IP address won't appear in the Port Access *Status and Operation* List. This setting is optional.

2. When you have finished with this page, click **Save**. You return to the Device List page. The Generic Device now appears in the list and in the Sidebar.

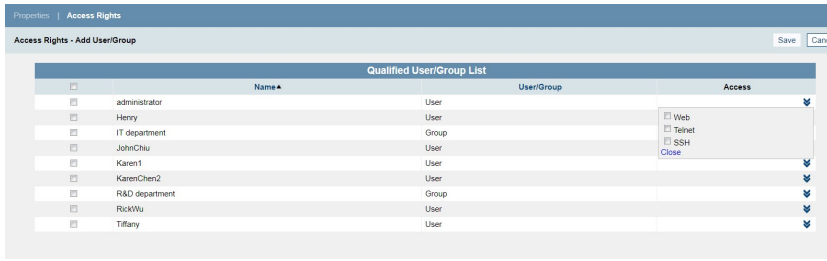
To give users and groups access rights to the device, do the following:

1. Select the newly added Generic Device in the main panel or the Sidebar, then select *Access Rights* on the Panel Menu bar. The User/Group List page comes up.

2. Click **Add** (at the top-right of the panel). The *Qualified User/Group List* page appears, listing the users who can be given access rights to the device:



3. Put a check in the box if front of the user or group name, then click the arrow at the right of the Access column to drop down a list of access rights choices.



4. Put a check in front of the rights you want the user or group to have, then click **Save** (at the top-right of the panel). You return to the Device List page. The Generic Device now appears in the list and in the Sidebar.

Note: The items that appear in the access rights panel depend on the settings choices that were made when the generic device was created (see *Network Information*, page 92).

■ Adding a Group Device

When you select *Group Device* as an item to be added, the *Add Group Device* page comes up. The procedure for adding Group Devices is essentially the same as that for adding Aggregate Devices. Follow the steps described in that section to add a Group device and assign ports to it.

Note: 1. Refer back to *Group Device*, page 83, for an explanation of the differences between Aggregate and Group devices.

2. A port can belong to any number of Group devices. When a port is made part of a Group Device it retains the locked/unlocked status of the original physical port. If you lock or unlock any of these ports, all the ports – including the original physical port – change to the new locked/unlocked status,

Modifying Devices

To modify a device's settings, do the following:

1. Select **Devices** either in the Sidebar (if it is available), or on the main menu bar (the orange bar).
2. Select the device you want to modify either from the Sidebar list, or in the main panel list.

3. Make your changes using the links that become available on the Panel Menu bar (the black bar). See *Sidebar Device Configuration*, page 105 for details concerning these Panel Menus.

Deleting Devices

To delete a device, do the following:

1. Select **Devices** either from the Sidebar list, or on the main menu bar (the orange bar).
2. Click to put a check in front of the device you wish to delete.

> **Note:** You can delete more than one device by checking as many of them as you require. You can delete all of them at once by checking the box at the top of the column.

3. After you have made your selection, click **Delete** (at the top-right of the panel).
4. In the confirmation popup that appears, click **OK**.

> **Note:** When you delete an Aggregate Device, all of its ports return to their original physical devices with their status changed to locked.

Deleting Unused Nodes

All unused nodes can also be deleted from the sidebar. To delete an unused node, do the following:

1. In the **Device** tab, select the node in the sidebar, and click **Delete** (at the top-right of the panel).

> **Note:** Only detachable nodes, such as dongles, PN stations, etc., can be deleted in this way; outlets cannot.

Detached Devices

In addition to the device types described above, there is another category of device, a *Detached Device*, which represents devices or ports that have been detected to have some sort of conflict with other valid devices or ports.

Examples:

1. On a NetDirector AXS managed KVM switch, if there are Adapter Cables connected to ports 4 and 6, and you remove the adapter from port 4, the NetDirector AXS will assume that the device connected to port 4 is off line.
2. If on the NetDirector AXS managed KVM switch you unplug the adapter cable from port 6 and plug it into port 4, the cable's Adapter ID will not match the device information for port 4 stored in the NetDirector AXS' database. The NetDirector AXS will recognize the new Adapter ID for port 4 and will treat the original port 4 Adapter ID as a detached device.
3. If you plug the Adapter Cable originally connected to port 4 in *Example 2*, into any other port on the KVM switch, the 4 and will treat will recognize the cable's Adapter ID and update its database accordingly, and the cable will not be treated as a detached device.

Detached devices can be found at the bottom of the tree. You can look at the device to try to resolve the conflict. Detached devices that haven't been resolved within 10 days are automatically removed.

Locking / Unlocking Ports

When physical devices are added to the NetDirector AXS management system, their ports are locked by default – to make a port available, it must be unlocked. When a port is selected, two buttons appear at the top-right of the Port Properties page: *Lock* and *Unlock*. To unlock a port, select it in the Sidebar or Interactive Display Panel, and click **Unlock**.

The ability to lock and unlock ports allows you to have pre-configured device nodes set up on your installation that are in excess of the amount licensed. If the total number of device nodes on the installation exceeds the number you have been licensed for, you can choose which device nodes to exclude by selecting them and clicking **Lock**. You can utilize them when necessary by locking different ones to create room, and then unlocking them.

Note: Ports are automatically unlocked when they are added to an Aggregate Device, but if you only want to use one or two of the device's physical ports, it is not necessary to go through the procedure involved in creating an Aggregate Device to do so. Simply select the target port(s) and click **Unlock**.

Locking / Unlocking Devices

When physical devices are added to the NetDirector AXS system, their ports are locked by default – to make a port available, it must be unlocked. You can lock/unlock all ports on a device using the buttons described below.

The **Lock**, **Unlock**, and **Unlock All** buttons are found at the top of the *Devices* page and on each Device's Properties page. The buttons allow you to lock and unlock all ports on the selected device. When a locked device is expanded from the sidebar, all ports will appear with an **X**. To lock and unlock individual ports see the *Locking / Unlocking Ports* section above for details.

To lock or unlock a device, select the device(s) from the *Devices* main page by checking the box; or click the device from the sidebar; and click the **Lock** or **Unlock** button.

Using the **Unlock All** button will unlock all devices on the NetDirector AXS - from top to bottom, until the available node licenses run out.

Transfer Device Settings

The **Transfer** button is found at the top of each device's Properties page. The button allows you to transfer the device settings and access rights from the selected device to another. After clicking the Transfer button a page appears displaying the available devices (the model must be the same) to transfer the settings to. Choose a device by selecting the radio button and click **OK**. An alert will appear asking you to confirm the transfer. The NetDirector AXS will transfer all device settings (excluding Device ID, model name and port number) and access rights to the device. The transfer does not affect the settings of the source device and it only applies to the device/dongle with the same model name and physical location (port); unmatched port/dongle settings and access rights will be ignored.

Tools

When you click *Tools* on the Panel Menu bar, the following page comes up:



Clicking an icon performs a specific task. The task that each of the icons performs is described in the table, on the next page.

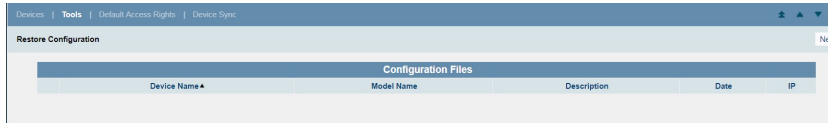
Icon	Task
	**Broadcast IP address and port number to the devices:** Before a device can communicate with the NetDirector AXS, its ANMS settings have to specify the NetDirector AXS' IP address and device management port number. Clicking this icon causes the NetDirector AXS to broadcast its IP address and device management port number to the devices connected to it on its network, which automatically sets them on the devices (instead of having to set them manually on the device, itself). This is done the first time that you connect a device to the ND network, or if a device has been reset to its default settings. **Note:** 1. This function uses UDP to broadcast the information. Therefore the devices must be on the same network segment (VPN will not work). UDP uses port 18768 – make sure that the network settings for computers that the NetDirector AXS is installed on have this port open. 2. For heightened security, once the broadcast is done and the information has been sent to the device, the device will not accept UDP broadcasts from any other NetDirector AXS. 3. If you change NetDirector AXS, you must use the ANMS settings page to specify the IP Address and port number (see *Device Configuration (For KVM Devices)*, page 112).
	**Broadcast changed IP address and port number to the devices:** This feature is used when the NetDirector AXS' IP address and/or device management port number changes. Clicking this icon causes the NetDirector AXS to broadcast its new IP address and/or device management port number to the devices connected to it on its network – automatically updating their ANMS settings accordingly. **Note:** 1. This function uses UDP to broadcast the information. Therefore the devices must be on the same network segment (VPN will not work). 2. For heightened security, the receiving devices will only accept UDP broadcasts from the NetDirector AXS that originally initialized them.

Icon	Task
	Restore device configuration: This feature is used to restore a device's configuration and/or account information to one saved on a previously backed up configuration file (See *Backup Device Configuration/Account Information*, page 141). See the section, below, for the restoration procedure.
	Device Name Sync: If device name changes have taken place, this feature is used to manually sync the names between the devices and the NetDirector AXS. See *Default Access Rights*, page 103 for automatic syncing details.

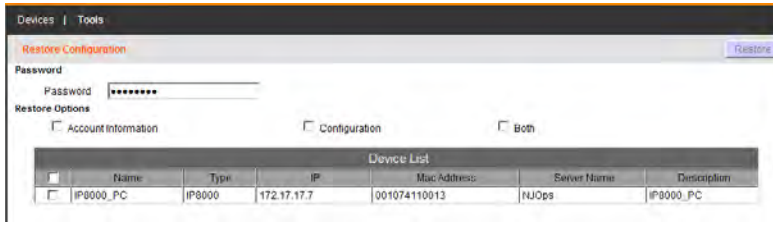
Restoring Device Configurations

To restore a device's configuration and/or account information to one saved on a previously backed up configuration file, do the following:

1. In the Device Management → Devices → Tools, Panel Menu, click **Restore device configuration**. A list of saved configuration files comes up:



2. Select the file you would like to restore, then click **Next**. The Restore Configuration page comes up:

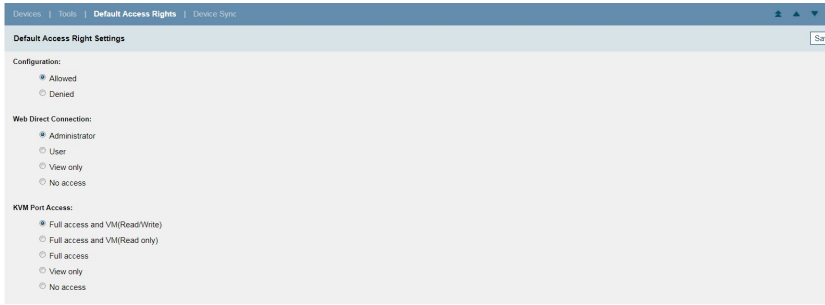


3. Key the password you used when the file was created in the *Password* field.
4. Click the appropriate checkbox to restore only the device account information; only the device configuration settings; or both.
5. Click the checkbox in front of the name of the device you want to restore, then click **Restore**.

   When the restoration is complete, a message appears informing you of the result.

Default Access Rights

The *Default Access Rights* page allows you to set the default access rights for all new devices added to the NetDirector AXS installation.



Device Sync

When you click *Device Sync* on the Panel Menu bar, the following page comes up:



This page lets you configure automatic syncing of names between the NetDirector AXS and the installed devices. Check the boxes for the features you want to enable, then click **Save**.

Sidebar Device Configuration

Certain aspects of a device's configuration are established when the device is created. There are additional settings for managing your devices that become available when you select a device item in the Sidebar or from the Device List in the main panel.

Clicking a device item in the Sidebar or from the Device List in the main panel invokes several Panel Menu items that allow you to refine the device item's configuration settings. The items offered, as well as the setting items offered under the Panel Menus, vary depending on which device is selected. An explanation of the Panel Menus and their settings is provided in the sections below.

Note: Access rights can be configured on an individual, port-by-port, basis. Giving a user access and configuration rights to a device does not necessarily mean giving the user rights to every port on the device.

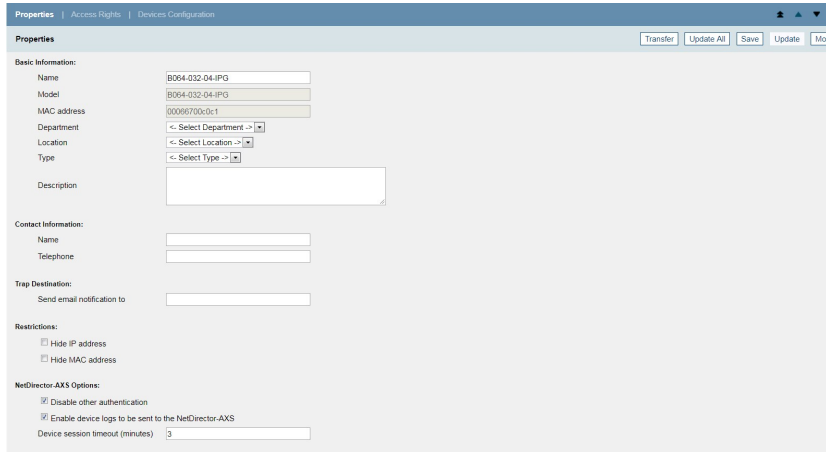
KVM Devices and Ports

Selecting a KVM device, such as the B064 series or other compatible models , or one of its ports, brings up a page with two entries on the Panel Menu bar: Properties, and Access Rights. Each of these items is discussed as following:

Properties

The settings found on the *Properties* page for devices are similar to the ones described in the *Adding Devices* section. See the table on page 87, for details.

The Port Properties page looks similar to the screen shown below:



An explanation of the property items is given in the table, below:

Item	Explanation
Basic Information	**Name:** Provide a name to identify the port. The default is the port name it was given under its original device configuration. If you change the name here, the change only takes place in the NetDirector AXS database. The name on the original configuration remains. **Model:** The NetDirector AXS recognizes the device model and fills in this field automatically. It cannot be edited. If the device is a Cat5e KVM switch, the KVM Adapter Cable model displays here. **Port ID:** Port IDs are unique and permanent – they cannot be edited. The NetDirector AXS fills in this field automatically. For Cat5e KVM switch ports, the ID is derived from the KVM Adapter Cable ID. **Port Number:** The NetDirector AXS ascertains which port on the KVM switch is the one being configured and fills in this field automatically. It cannot be edited. **Department:** For organizational purposes you can establish department categories (R&D, for example), and assign ports to them. If you wish to assign this port to a department, drop down the list of departments (you have previously created – see *Departments, Locations and Types*, page 115), and click on the one you want the port to belong to. **Location:** For organizational purposes you can establish location categories (West Coast, for example), and assign ports to them. If you wish to assign this port to a location, drop down the list of locations (you have previously created – see *Departments, Locations and Types*, page 115), and click on the one you want the port to belong to. **Type:** For organizational purposes you can specify the type of device that this is. If you wish to do so, drop down the list of types (you have previously created – see *Departments, Locations and Types*, page 115), and click on the one you want. **Description:** If you wish to provide extra information to describe the port, enter it here. This field is optional.
Contact Information	The name and telephone number of the device administrator. These fields are optional.
System Macro	If system macros have been made, drop down the list to select the one you want. When you close the KVM viewer the macro will be sent to the server connected to this port and the server will run it. **Note:** This item only appears on ports that have servers connected to them.

Properties Page Action Buttons

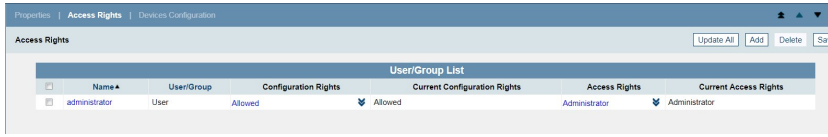
When a top-level (non-nested) Tripp Lite device is selected in the Sidebar or the Interactive Display Panel, a series of action buttons appear at the top-right of the Interactive Display Panel. The purpose of these buttons are explained in the following table:

Button	Purpose
Update All	Clicking this button brings up a page listing all of the items nested underneath the top-level device. This page allows you to configure (or reconfigure) the Department, Location, Type, and Description of each nested (child) item.
Lock All	If the total number of device nodes on the installation exceeds the number you have been licensed for, you can choose which device nodes to exclude by locking them. Click this button to lock all of the device's ports. See *Locking / Unlocking Ports*, page 99 for more information.
Unlock All	If any of the device's ports have been locked, click this button to unlock all of them.
Save	If you make any changes on the Properties page, click **Save** to save them and move on.
Update	If the installation information for a device doesn't match the information for it stored in the NetDirector AXS' database – for example, if an adapter is moved to a different port, or a new adapter is connected to a port – a question mark is added to its icon in the Sidebar and the *Update* button is enabled. Selecting the device in the Sidebar and clicking **Update** causes the NetDirector AXS to update the device's installation information in its database.
Move	Click this button to move the device into a different folder. Select the target folder in the dialog box that comes up, then click **OK**.

When a port is selected only the *Lock*, *Unlock* and *Save* buttons appear at the top-right of the page. These buttons allow you to lock and unlock the ports individually. See *Locking / Unlocking Ports*, page 99 for more information.

Access Rights – KVM Devices

When a KVM device is selected in the Sidebar or the Interactive Display Panel, you can set the configuration and access rights for it by clicking the *Access Rights* Panel Menu item. Clicking this item brings up a page that shows a list of all the users and groups that have been given access to it.



■ Adding Users or Groups to the Device User/Group List

To give a user or group access to the device, do the following:

1. Click **Add**. A list of qualified users and groups appears.
2. Click to put a check in the checkbox in front of the names of the users or groups that you want to access the device or port.
3. Set the configuration rights for the users or groups:
   - **Allowed** – The user or group can configure the device's settings.
   - **Denied** – The user or group cannot configure the device's settings.
4. Set the access rights for the users or groups:
   - **Administrator** – When accessing the device, the user or group has administrator privileges on it (according to the device's authorization policy).
   - **User** – When accessing the device, the user or group has user privileges on it (according to the device's authorization policy).
   - **View Only** – When accessing the device, the user or group can only view its ports – they cannot perform any actions on them.
   - **No Access** – The user or group cannot access any of the device's ports.
5. When you have finished making your configuration rights settings, click **Save**. The new users and groups are added to the device's User/Group list.

■ Modifying a User's or Group's Rights

To modify a user's or group's rights to the device, do the following:

1. In the *Configuration Rights* column that corresponds to the user or group you want to modify, click on the arrow; make your new selection; then click **Close**.
2. In the *Access Rights* column that corresponds to the user or group you want to modify, click on the arrow; make your new selection; then click **Close**.
3. click **Save** (at the top-right of the panel).

■ Deleting a User's or Group's Rights

To remove a user's or group's rights to the device, do the following:

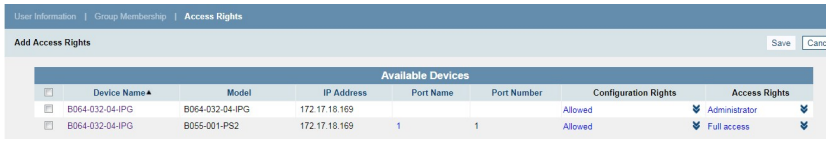
1. Click to put a check in the checkbox in front of the names of the users or groups that you want to remove.
2. Click **Delete** (at the top-right of the panel).

■ Action Buttons

In addition to Add, Delete, and Save, there is an *Update All* button (at the top-right of the panel). Clicking that button takes you to a page that lets you set the configuration and access rights for all users and groups on the selected device or port.

Access Rights – KVM Ports

When a port is selected in the Sidebar or the Main panel list you can set the rights for which users will be allowed to configure and access it by clicking the Access Rights Panel Menu item. Clicking this item brings up a page that shows a list of all the users and groups that have been given access to it.



■ Adding Users or Groups to the Port User/Group List

To give a user or group access to the port, do the following:

1. Click **Add**. A list of qualified users and groups appears.
2. Click to put a check in the checkbox in front of the names of the users or groups that you want to access the port.
3. Set the configuration rights for the users or groups:
   - **Allowed** – The user or group can configure the port's settings.
   - **Denied** – The user or group cannot configure the port's settings.

   Note: This setting is only available with ports on Cat5e KVM switches.
4. Set the access rights for the users or groups:
   - **Full access and VM (Read / Write) / Read Only**– The user can view the remote screen and can perform operations on the remote system from his keyboard and monitor. The user has read/write or ready only rights to use the virtual media function.

     Note: This setting is only available on B064-016-02-IPG, B064-032-02-IPG,B064-016-04-IPG, B064-032-04-IPG switches.
   - **Full access** – The user can view the remote screen and can perform operations on the remote system from his keyboard and monitor.
   - **View only** – The user can only view the remote screen; he cannot perform any operations on it.
   - **No access** – The port does not appear in the user's Port Access Sidebar or Status and Operation List (see *Port Access*, page 34).
5. When you have finished making your access rights settings, click **Save**. The new users and groups are added to the port's User/Group list.

■ Modifying a User's or Group's Rights

To modify a user's or group's rights to the port, do the following:

1. In the *Configuration Rights* column that corresponds to the user or group you want to modify, click on the arrow; make your new selection; then click **Close**.
2. In the *Access Rights* column that corresponds to the user or group you want to modify, click on the arrow; make your new selection; then click **Close**.
3. click **Save** (at the top-right of the panel).

■ Deleting a User's or Group's Access Rights

To remove a user's or group's access rights to a port, do the following:

1. Click to put a check in the checkbox in front of the names of the users or groups that you want to remove.
2. Click **Delete** (at the top-right of the panel).

■ Action Buttons

In addition to Add, Delete, and Save, there is an *Update All* button (at the top-right of the panel). Clicking that button takes you to a page that lets you set the configuration and access rights to the port for all users and groups.

Copy-Paste Access Rights

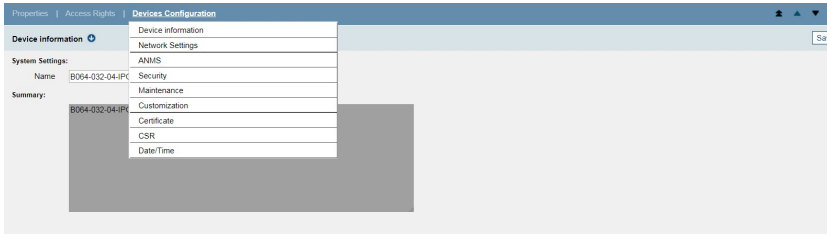
The access rights copy-paste function is enabled between compatible nodes (i.e. outlet to outlet). To use this function, in the sidebar tree, right-click on an outlet and select copy access right. Right-click on another outlet and select paste access right.

Device Configuration (For KVM Devices)

The purpose of Device Configuration is to allow you to configure the device from within the NetDirector AXS, without having to access the devicedirectly. Changes on these pages actually get made on the device, itself.

Note: If the link between the NetDirector AXS and the device should be broken for some reason, device configuration changes made on these pages will not be transmitted to the device. To make device configuration changes you can log in to the device directly

This Panel Menu item contains several secondary pages. To modify the information on these pages, you can either move through them sequentially, by clicking the arrow icons (and) at the left of the main panel in the gray bar, or you can go directly to a page by hovering over the menu and selecting the page from the popup menu that appears.



Note: The Device Configuration Panel Menu doesn't appear if the device is offline

The secondary Panel Menu pages correspond to the administration functions described in the device's User Manual. For configuring the settings, refer to the manual's Device Management chapters to obtain the necessary information. When you have finished making your configuration settings, click **Save**.

Note: 1. On the NetDirector AXS' secondary Panel Menu ANMS settings page, in addition to the entry labeled *Preferred ND Server Settings*, there is an entry called *Alternate ND Server Settings*. The Preferred settings correspond to the ANMS settings on the device Changes to this setting take place on the device.

2. On the NetDirector AXS' secondary Panel Menu Customization settings page, there is an entry called *Port timeout*. This field sets a time threshold for users on ports whose Access Mode has been set to *Occupy* (see *Mode*, page 114).

   This corresponds to the *Access Mode* setting on the original device. If there is no activity from the useroccupying the port for the amount of time set here, the user is timed out and the port is released. The first user to send keyboard or mouse input after the port has been released gets to occupy the port.

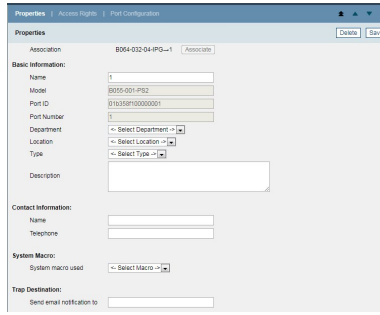
   Input a value from 0 to 255 seconds. The default is 3 seconds. A setting of 0 causes the port to be released the instant there is no input.

Port Configuration (For Cat5e KVM Devices)

The purpose of Port Configuration is to allow you to configure the port from within the NetDirector AXS, without having to access the device directly. Changes on these pages actually get made on the device, itself.

Note: If the link between the NetDirector AXS and the device should be broken for some reason, device configuration changes made on these pages will not be transmitted to the device. To make device configuration changes you can log in to the device directly

This Panel Menu page is used to set the I/O attributes of the selected port:



The meanings of the attribute headings are described in the table, below:

Heading	Meaning
Port Name	This is the name given to the port.
Exit Macro	If system macros have been made, drop down the list to select the one you want. When you close the KVM viewer the macro will be sent to the server connected to this port and the server will run it.
Cable	Specifies the length of the Cat5e cable that is used to connect the computer to the port.
OS	Specifies the operating system that the computer on the connected port is using.
Language	Specifies the OS language being used by the computer on the connected port.
Mode	This corresponds to the Access Mode setting on the original device (Share, Occupy, Exclusive). It defines how the port is to be accessed when multiple users have logged on. **Exclusive:** The first user to switch to the port has exclusive control over the port. No other users can view the port. The *Timeout* function does not apply to ports which have this setting. **Occupy:** The first user to switch to the port has control over the port. However, additional users may view the port's video display. If the user who controls the port is inactive for longer than the time set in the *Timeout* box, port control is transferred to the next user to move the mouse or strike the keyboard. **Share:** Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically.

To configure the settings, refer to the device's User Manual to obtain the necessary information. When you have finished making your configuration settings, click **Save**.

Departments, Locations and Types

For convenience, and ease of management, the *Departments*, *Locations*, and *Types* pages provide three more ways of organizing your devices. To use this organizational scheme, you would first create appropriate categories (such as *R&D* and *Manufacturing* under Departments; *East Coast Operations* under Locations; and *Power* under Types), and then assign devices to them (from the device's Properties page), as described in the sections that follow.

Adding a Department Location or Type

To create a Department, Location, or Type, do the following:

1. Select **Department**, **Location**, or **Type** on the Menu Bar. The *Department*, *Location*, or *Type* List page comes up:



2. Click **Add** (at the top-right of the panel). The Add Department (or Location or Type) page comes up:



3. Fill in the Name and Description fields, then click **Save**.

Assigning Devices and Ports

To assign a device or port to a Department, Location, or Type, do the following:

1. Select **Devices** on the Menu Bar.
2. In the Sidebar, select the device or port you want to assign to a Department, Location, or Type. Its *Properties* page comes up (see page 93).
3. Drop down the list of Departments, Locations, or Types and click on the one(s) you want the device or port to belong to.

Modifying a Department, Location, or Type

To change the name or description of a Department, Location, or Type, do the following:

1. Select **Department**, **Location**, or **Type** on the Menu Bar.
2. In the Sidebar or Main Panel, select the Department, Location, or Type you want to modify.
3. On the Panel Menu bar, select **Properties**.
4. Make your changes, then click **Save**.

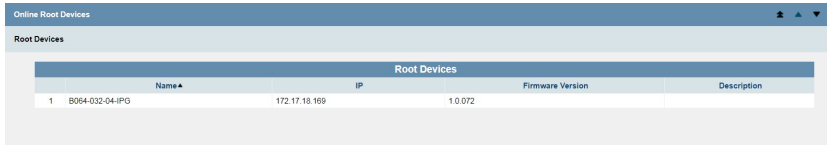
Deleting a Department, Location, or Type

To delete a Department, Location, or Type, do the following:

1. Select **Department**, **Location**, or **Type** on the Menu Bar. The *Department*, *Location*, or *Type* List page comes up.
2. Click to put a check mark in front of the name of the Department, Location, or Type you wish to remove, then click **Delete** (at the top-right of the panel).

Online Devices Information

The *Online Devices Information* tab is a convenient way to view information of devices that are being managed by the NetDirector AXS. Clicking in the tab brings up a list of devices/dongles deployed in the installation and displays their IP address and firmware version, as shown below:



Note: 1. This is a view-only tab – no actions can be performed.

2. The Root Devices list is sortable by Name, Type, and IP

Unsupported Devices

Unsupported devices are Tripp Lite devices whose firmware level is not compatible with the NetDirector AXS' current firmware level. Clicking *Unsupported Devices* on the Menu Bar brings up a page that lists all such devices deployed on the NetDirector AXS installation:



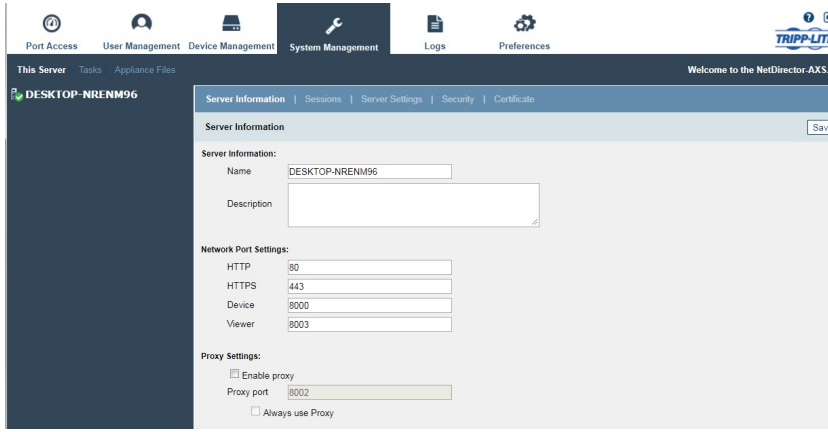
To make these devices available for management under the NetDirector AXS, their firmware must be upgraded to the latest version. To do this, contact Tripp Lite Product/Technical Support.

Once the firmware upgrade completes, the device is removed from the Unsupported Devices list, and now appears in the Available Devices list (see *Adding a Folder or Device*, page 91).

Chapter 7
System Management

Overview

A NetDirector AXS installation is comprised of NetDirector AXS compatible devices residing on a network segment that are connected – over-IP – to a NetDirector AXS server that also resides on that same network segment. By connecting NetDirector AXS server segments through IP addresses into an integrated worldwide network, theNetDirector AXS provides secure, centralized, single IP address login access, to all your data center equipment from anywhere there is an internet connection, at any time.



Note: The System Management page is for System Administrators. Other user types can omit this chapter.

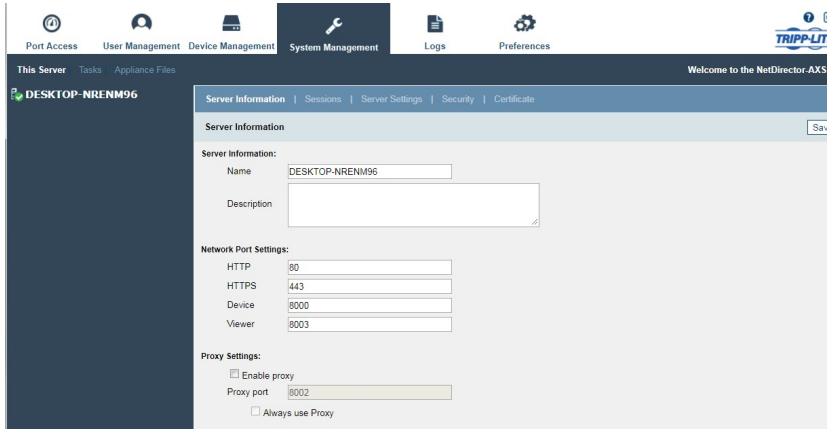
This Server

The *This Server* Page Menu refers to the NetDirector AXS you are currently logged into.
The menu offers five Panel Menu choices: Server Information, Server Settings, Security, and Certificate.

Note: Changes to other servers on the installation can only be made by logging into them directly.

Server Information

The default page is Server Information, and looks similar to the one below:



This page allows you to configure the NetDirector AXS server's settings. The meanings of the field headings are described in the table, below:

Field	Description
Name*	You can change the NetDirector AXS server's name by editing this field.
Description	You can change NetDirector AXS server's description by editing this field. The description can be from 2–32 Bytes in any supported language.
HTTP*	The port that the NetDirector AXS uses to communicate with browsers.
HTTPS*	The secure port that the NetDirector AXS uses to communicate with a browser over the internet.
Device Port*	The port that the NetDirector AXS uses to communicate with devices on the installation.
Viewer Port	The port that the NetDirector AXS uses for the viewers to communicate with when Multiviewer is in effect. See *Launch Multiviewer*, page 36.
Enable Proxy	When using the proxy function, check this box, then specify the proxy port in the indicated field. See *NetDirector AXS Proxy Function*, page 167.
Location	Choose whether you want to specify the server's location by its address, or by its coordinates, then fill in the appropriate address or latitude and longitude information in the indicated fields. Click the *Map* button to bring up a navigable world map, then click on the appropriate spot on the map to set the location.

***** See page 13 for details.

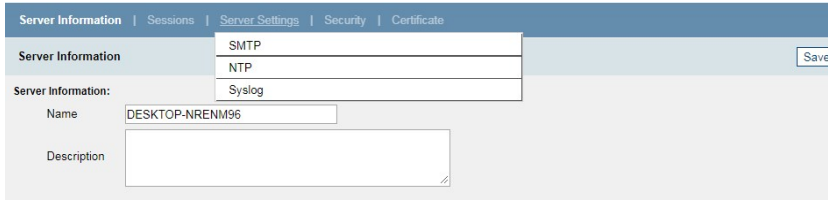
When all your configuration settings have been made, click **Save**.

Sessions

In the Sidebar, lists all the sessions currently taking place on NetDirector AXS on the installation, and provides information concerning the "who, where and when" of each.

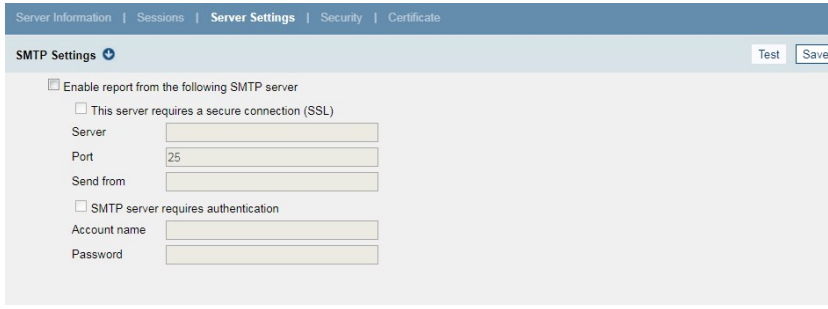
Server Settings

To modify the information on these pages,
you can either move through them sequentially, by clicking the arrow icons (and) at the left of the main panel in the gray bar, or you can go directly to a page by hovering over the menu and selecting the page from the popup menu that appears.



SMTP

The NetDirector AXS can send email notification of event traps on the installation to specified users.



Note: Event notification recipients are designated on the The *Notification Settings* page. See page 151 for details.

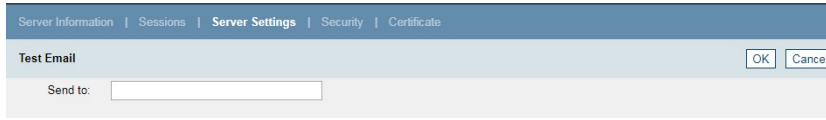
To enable SMTP server setting, do the following:

1. Check the *Enable report from the following SMTP server* checkbox.
2. Specify the IP address or domain name of the computer running your SMTP server in the *Server* field.
3. Specify the port number that the SMTP server listens on.

4. Specify the NetDirector administrator's email address in the *Send from* field.

Note: This field cannot be blank.

5. If the SMTP server requires authentication, check the *SMTP server requires authentication* checkbox, then specify the authentication account name and password in the appropriate fields.
6. In the *Language* field, specify the language for the email notification in the drop-down menu.
7. Click **Test** to check that the SMTP server setting is configured properly. A screen similar to the one below appears:



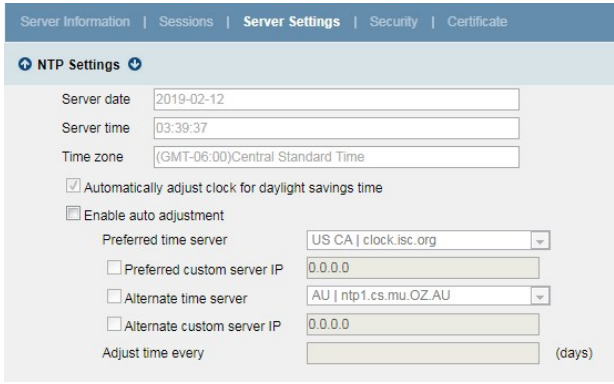
8. Key in an email address for the recipient of the test email then click **OK**. If the settings have been configured correctly, the recipient will receive the test email.

Note: The email address of the recipient cannot exceed the equivalent of 128 English alphanumeric characters.

9. Click **Save** to complete the procedure.

NTP

The NTP page lets you have the NetDirector AXS' time automatically synchronized to a network time server:



Note: 1. The top three fields are filled automatically by the NetDirector AXS, and can't be edited.

2. If you are in a timezone that doesn't have daylight savings time, the *Automatically adjust clock for daylight savings time*, checkbox is disabled.

To have the NetDirector AXS' time automatically synchronized to a network time server, do the following:

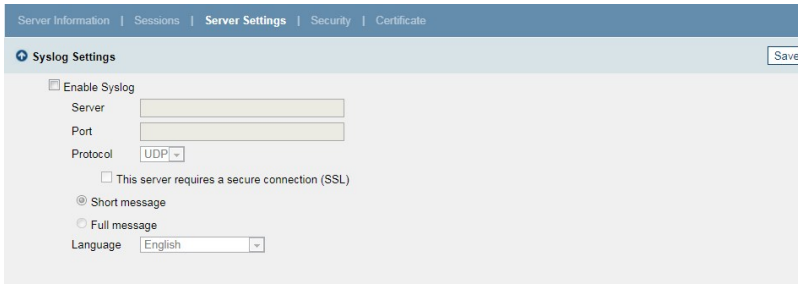
1. Check the Enable auto adjustment checkbox.
2. Drop down the time server list to select your preferred time server

   – or –

   Check the Preferred custom server IP checkbox, and key in the IP address of the time server of your choice.
3. If you want to configure an alternate time server, check the *Alternate time server* checkbox, and repeat step 2 for the alternate time server entries.
4. Key in your choice for the number of days between synchronization procedures.
5. If you want to synchronize immediately, click **Adjust Time Now**.

When all your settings have been made, click **Save**.

Syslog



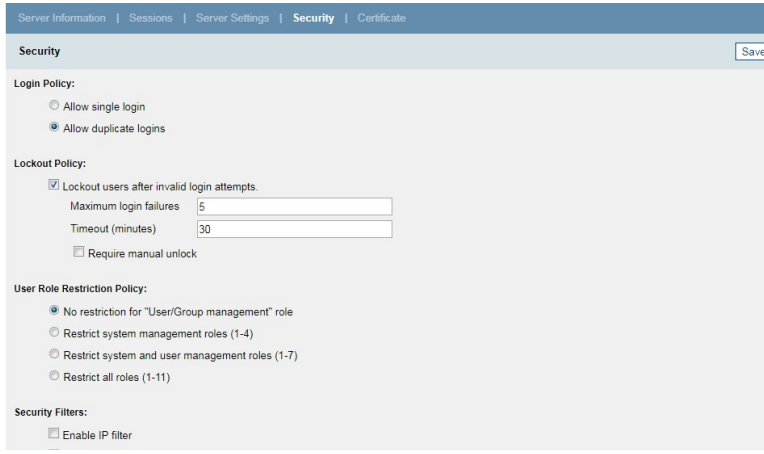
To record all the events that take place on the NetDirector AXS and write them to a Syslog server, do the following:

1. Check **Enable**.
2. Key in the IP address and the port number of the Syslog server. The valid port range is 1-65535.
3. Select whether to log a short message or a full message.
4. Drop down the list to select the language you want the message sent in.

When all your settings have been made, click **Save**.

Security

This page provides a level of security by controlling access to NetDirector.



Login Policy

- Select **Allow single login** if you don't want users to be able to log in more than once at the same time.
- Select **Allow duplicate logins** if you want users to be able to log in with the same account more than once at the same time. This is the default.

Lockout Policy

- To lock users out after a specified number of failed login attempts, click to put a check in the *Lockout users after invalid login attempts* checkbox enable the lockout function. The default is enabled.

> **Note:** If you don't check this box, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, we recommend that you enable the lockout policy.

- Key the number of login failures you wish to allow before the user gets locked out in the *Maximum login failures* field. The value specified here must be at least 1. The default is 5.
- Key the amount of time (in minutes) a locked out user must wait before being allowed to log in again in the *Timeout* field. The value specified here must be at least 1. The default is 30.
- Enabling *Require manual unlock*, means that users will not be able to log in after their account has been locked until they contact an administrator to have the administrator manually unlock the account. See *Unlocking User Accounts*, page 65, for details. The default is disabled (no check in the checkbox).

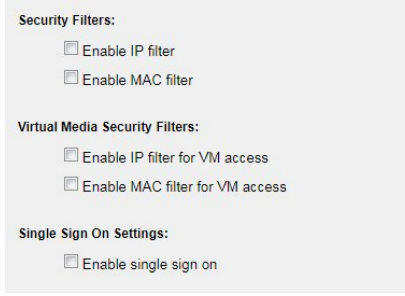
IP Filtering

IP filtering controls access to the NetDirector AXS based on the IP addresses of the computers attempting to connect to it.

- To enable IP filtering, check the Enable IP Filter checkbox. If the Include button is selected, all the addresses specified in the Address List are allowed access; all other addresses are denied access. If the Exclude button is selected, all the addresses specified in the Address List are denied access; all other addresses are allowed access.
- IP filters can consist of a single address, or a range of addresses. You can add as many IP addresses as you require. Key the addresses directly into the IP address text input box as follows: For multiple single address entries, use a comma between the IP addresses. There is no space before or after the commas. For a range of filters, key in the starting IP address, followed by a dash, then the ending IP address.
- To modify or delete a filter, make your changes directly in the IP address text input box.

MAC Filtering

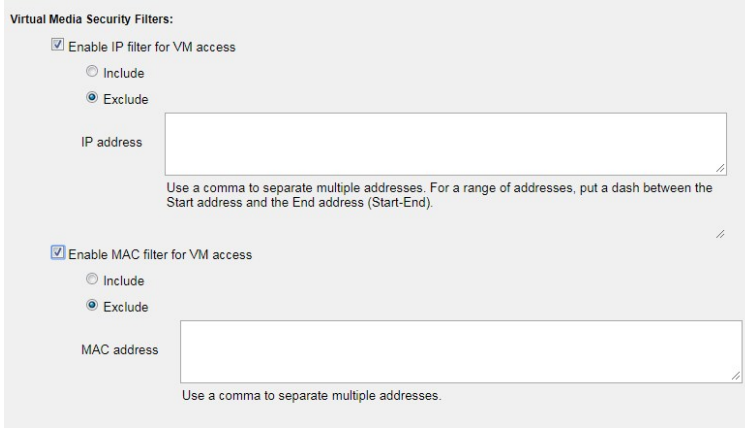
MAC filtering controls access to the NetDirector AXS based on the MAC addresses of the computers attempting to connect to it.



- To enable MAC filtering, check the *Enable MAC Filter* checkbox. If *Validate MAC at NetDirector AXS login* is enabled, the NetDirector AXS will verify the client PC's MAC address when the user attempts to log in. Otherwise, the MAC address will only be verified when attempting to open a viewer. If the *Include* button is selected, all the addresses specified in the address list are allowed access; all other addresses are denied access. If the *Exclude* button is selected, all the addresses specified in the address list are denied access; all other addresses are allowed access.
- MAC filters can consist of a single address, or a range of addresses. You can add as many MAC addresses as you require. Key the addresses directly into the IP address text input box, using a comma between the addresses. There is no space before or after the commas.

Virtual Media Security Filters

IP and MAC filtering can also be used to control Virtual Media access, based on the IP and MAC addresses of the computers attempting to use virtual media access.



- To enable virtual media security filters, check the *Enable IP filter for VM Access* and *Enable MAC filter for VM access* checkboxes and follow the instructions given in *IP Filtering* and *MAC Filtering* in page 128.

Single Sign On

If *Single Sign On* is enabled, users that are authenticated via the NetDirector AXS are automatically authenticated on all the devices deployed on the system. They don't have to be authenticated on each device individually.

Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the site he intended. The *Certificate* page is used to create, modify, or obtain a certificate for this purpose.

During installation, each NetDirector AXS creates its own, independent, self-signed certificate based on the installation information, similar to the one below:



Changing a Self-Signed Certificate

Changing a self-signed certificate allows you to provide additional information in the certificate that wasn't generated in the installation certificate. The way to change a self-signed SSL certificate is to create a new one. To create a new self-signed certificate, do the following:

1. At the top-right of the Certificate panel, click **Update**. The following page appears:



2. Select the *Create a new self signed SSL server certificate* radio button, then fill in the fields according to the information in the table below:

Field	Description
Common Name	This is the Fully Qualified Domain Name (FQDN) for which you are requesting the SSL certificate. For example: www.yourdomainname.com
Organization	This is your Full Legal Company or Personal Name, as legally registered in your locality.
Organizational Unit	The branch of your company that is ordering the certificate. For example: accounting, marketing, etc.
City or Location	Key in the full name of the city or location. For example: Chicago
State or Province	Key in the full name of the state or province.
Country	This is the two letter country code for the country where the organization that the certificate is being registered to is located. **Note:** These don't always correspond to common abbreviations. If you are not sure of the code, you can do an online search for **ssl+country codes**.

3. When you have finished filling in the fields, click **Save**.

   A message appears asking you to wait while the database gets updated with the new information. After a moment the web page closes.

   At this point you are brought back to the beginning of the login sequence where you must go through the procedure of accepting the security certificate and logging in.

Importing a Signed SSL Server Certificate

In order to avoid users having to go through the certificate acceptance prompt each time they log in, administrators may choose to use a third party certificate authority (CA) signed certificate.

To use a third party signed certificate, do the following:

1. After generating the self-signed certificate, click **Get CSR** (Certificate Signing Request) at the top-right of the panel.
2. Go to the CA website of your choice and apply for an SSL certificate using the information generated in step 1.
3. After the CA sends you the certificate, open the *Server Certificate* page, click **Update** at the top-right of the panel.
4. Select **Import a signed SSL server certificate**; then browse to where the certificate file is located and select it.
5. Click **Save** at the top-right of the panel.

Note: Each of the certificate types mentioned in this section provides an equal level of security. The advantage of the changed self-signed certificate is that it allows you to provide more information than the installation certificate. The advantage of a CA third party certificate is that users do not have to go through the certificate acceptance prompt each time they log in, and it provides the additional assurance that a recognized authority has certified that the certificate is valid.

Tasks

The Tasks menu allows authorized administrators to perform a number of system maintenance tasks. The tasks that can be performed are determined by the user's type, and the authorization options that were selected when the user's account was created. These include:

- Exporting event logs
- Upgrading the firmware of selected appliances
- Backing up device configuration and account information
- Exporting the device log
- Exporting the session history

When you open the Tasks page on a NetDirector AXS, a screen similar to the one below appears:



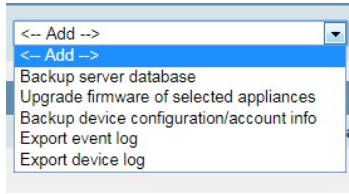
The *Task List* table lists all the tasks that have been configured. The meanings of the headings are explained in the table, below:

Heading	Explanation
Name	The name you gave to the task when you configured it.
Type	The type of task that it is.
Next Run	If the task is scheduled to be run at a certain time, the time that it will run appears here.
Last Run	Indicates the last time that the task ran.
Status	Indicates whether the task is running or is idle.

Adding a Task

To add a task, do the following:

1. Click the arrow at the right of the *Add* field to drop down the list of task choices:

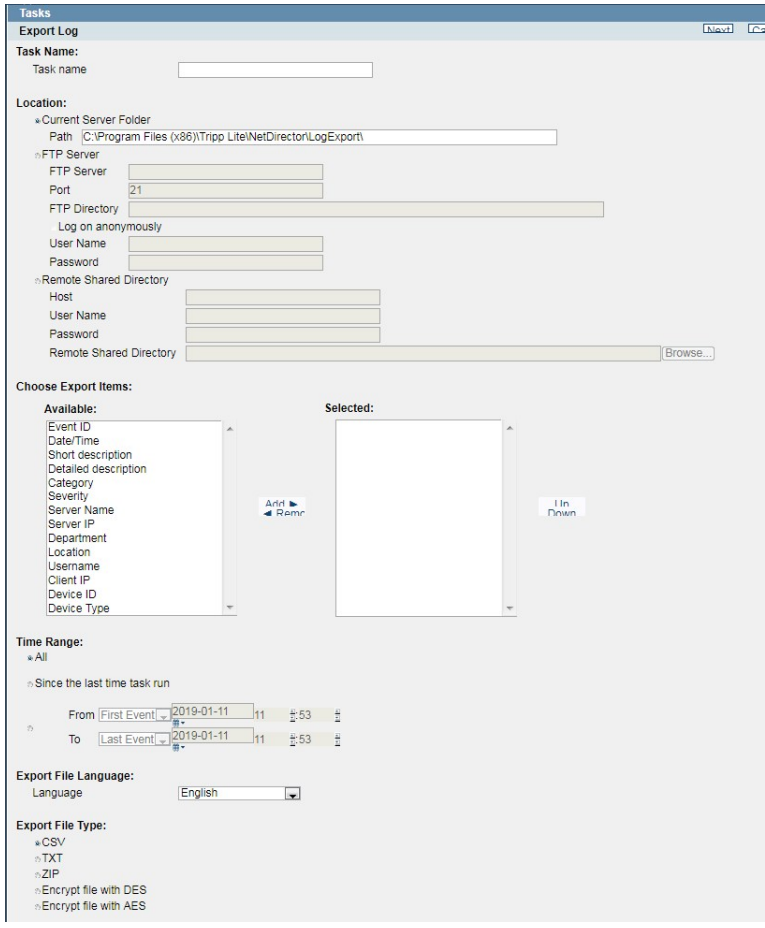


2. Click on the task you want to add.

Depending on the task you choose, a page comes up with various choices for you to make. While each of the tasks is different, for the most part the procedures involved in setting them up are similar. The following examples take you through the various task procedures you will encounter.

Export Event Log

When you choose the *Export event log* task, the following page appears:



1. Key in a name for the task in the *Task name* field.

   Note: The *Export Event Log* operation is performed on each server independently. To search a server's records you must look at its particular file. You can identify the file by means of the *Task name* you gave it.

2. Select the location where you want to store the exported file, and fill in the fields accordingly. The default setting is for the file to be exported to a directory on the current NetDirector AXS server: `C:\NetDirector AXS\NetDirector AXSLogExport`.
3. Select an item that you want to include in the exported file in the *Available* column, then click **Add** to move it into the *Selected* column. Repeat for any other log file items you want to include.

   Note: To select multiple items, use Shift+Click or Ctrl+Click.

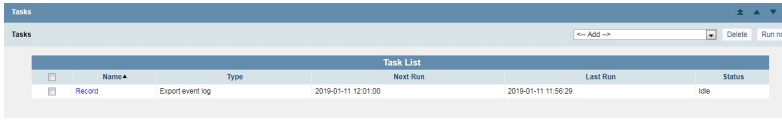
4. To change the order of the *Selected* items, click on the item you want to move, then click **Up** or **Down** to change it to the position you want.
5. For *Choose Export Period*, selecting **All** exports all the records in the database. To export records for a particular time period, select the radio button below it and set the time parameters with the *From* and *To* settings.
6. For *Export File Language*, choose **Default** to have the file exported in the language that your browser is set to. If you prefer a different language, drop down the list and select one of the languages offered.
7. For *Export File Type*, click the radio button in front of your choice. If you choose one of the encryption options (AES or DES), key a password into the *Password* field that comes up.

   Note: Make a note of the password – you will need it to import the file (see *Import Logs*, page 155, for details).

8. When you have finished with this page, click **Next** (at the top-right of the panel), to move on.
9. Make your schedule choices in the pages that come up.

10. When you have completed your schedule choices, click **Next**.

    The procedure completes and you return to the *Tasks* main page. The Export Event Log task, configured according to the choices you made, is now added to the Sidebar and the Task List:



Upgrade Selected Appliance Firmware

This task allows you to schedule the firmware upgrading of devices on your installation so that they can take place at the most convenient time.

When you choose *Upgrade Selected Appliance Firmware*, the following page appears:



To schedule the firmware upgrade of selected appliances, do the following:

1. Click a radio button to choose whether to use the latest upgrade file stored with the NetDirector AXS server, or to upgrade with a selected file that you have uploaded.

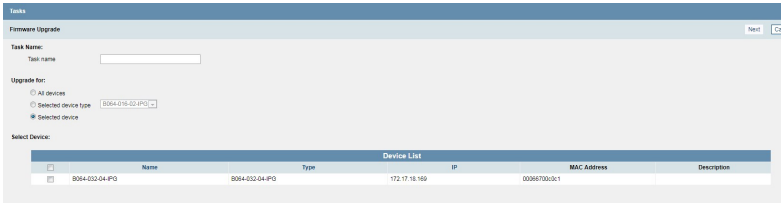
Note: 1. The files stored with the NetDirector AXS server, are the ones that came as part of its firmware. These are usually the latest versions that are compatible with NetDirector AXS. We recommend using them unless you have a particular reason for choosing a specific other one.

2. If you choose *Upgrade with a selected firmware file*, before upgrading, you must first upload the upgrade file. See *Firmware Files*, page 145, for details

---

2. If you choose *Upgrade with the latest stored version* (recommended), all the devices are automatically selected for the upgrade. If you choose *Upgrade with a selected firmware file*, click the button in front of the device type you want to upgrade.
3. Click **Next** (at the top-right of the panel).

   The *Firmware Upgrade* page appears:



4. Key an appropriate name to describe the task in the *Task name* field.

5. Click a radio button to select which appliances will receive the upgrade.
6. If you choose *Selected device type*, drop down the list and select the device type. Only those devices that are of the selected device type receive an upgrade.
7. If you choose *Selected device*, put a check in the checkbox in front of the devices you want to upgrade (or check the box at the top of the column to select them all).

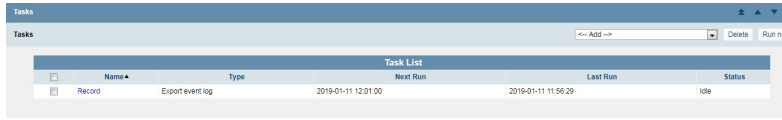
Note: 1. For KVM switches with Adapter Cables, click the arrowhead in front of the switch's name to select the Adapter Cable firmware you wish to upgrade.

2. The Device list is sortable by Name, Type, and IP.

---

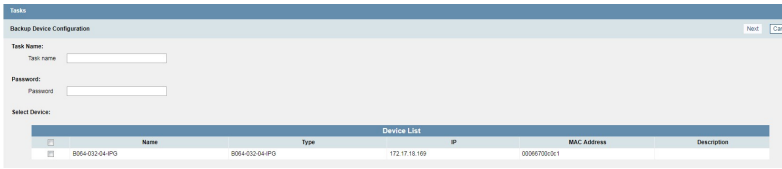
8. Click **Next**.
9. Make your schedule choices in the *Schedule* page that comes up.
10. When you have completed your schedule choices, click **Next**.

    The procedure completes and you return to the *Tasks* main page. The task is now added to the Sidebar and the Task List:



Backup Device Configuration/Account Information

When you choose the *Backup device configuration/account information* task, the following page appears:



1. Provide a name for the task and a password.

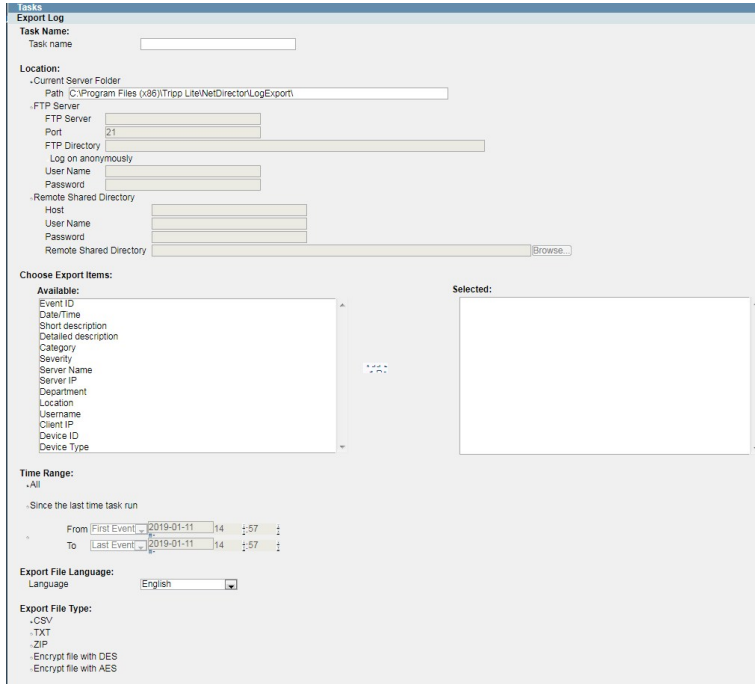
   Note: Make a note of the password and store it in a safe place. You will need it when restoring the configuration/account information. See *Restore device configuration*, page 102 for restoration details.

2. In the *Device List*, put a check in the box in front of the name of the device you want to back up, then click **Next**.
3. Make your schedule choices in the *Schedule* page that comes up.
4. When you have completed your schedule choices, click **Next**.

   The procedure completes and you return to the *Tasks* main page. The *Backup device configuration/account information* task, configured according to the choices you made, is now added to the Sidebar and the Task List:

Export Device Log

The NetDirector AXS acts as a log server for all supported Tripp Lite over IP KVM switches, recording the system events that take place on the devices in a database. This task allows you to write the contents of the device database to a file. When choosing the *Export device log* task, the following page appears:



1. Provide an appropriate name for the task. For example, if you want to export the device log for all supported KVMs you might name the task *All-B064-log*; if you want to export the device log for B064 series devices on a weekly basis, you might name the task b064-*weekly-device-log*.

Note: The *Export Device Log* operation is performed on each server independently and stored on each server independently. To search the records you must go to each server to look at its particular file.

2. Select the location where you want to store the exported file, and fill in the fields accordingly. The default setting is for the file to be exported to a directory on the current NetDirector AXS server.

   Note: The path to the directory on your server that will hold the backup file is pre-configured based on the directory that the NetDirector AXS was installed in. For example, C:\NetDirector AXS\LogBackup

3. You can use the *Pattern* field as a filter to limit the scope of the log file. For example, to export a file that only contains event information for B064 series devices, and all your B064 devices had B064 as part of their names, you would key **B064** into the Pattern field.

4. For the *Time Range*:
   - Selecting **All** exports all the records in the database.
   - To export records for a particular time period, select the **Include** radio button and set the time parameters with the *From* and *To* settings; To export all records that *do not* include a particular time period, select the **Exclude** radio button and set the time parameters that you do not want to include with the *From* and *To* settings.

5. For *Export File Type*, click the radio button in front of your choice. If you choose one of the encryption options (AES or DES), key a password into the *Password* field that comes up.

   Note: Make a note of the password – you will need it to import the file (see *Import Logs*, page 155, for details).

6. When you have finished with this page, click **Next** (at the top-right of the panel), to move on.

7. Make your schedule choices in the pages that come up.

8. When you have completed your schedule choices, click **Next**.

   The procedure completes and you return to the *Tasks* main page. The Export Event Log task, configured according to the choices you made, is now added to the Sidebar and the Task List.

Editing a Task

There are two editing tasks that you can perform: changing a task's schedule, and changing the parameters of what you want the task to perform.

- To change a task's schedule, do the following:
  1. Click on its name – either on the Sidebar or in the Task List.
  2. The *Schedule* page comes up. Make the schedule changes you want, then click **Save**.
- To change the parameters of what you want the task to perform, do the following:
  1. Click on its name – either on the Sidebar or in the Task List.
  2. The *Schedule* page comes up. Click **Task Properties** on the Panel Menu.
  3. When the Task Properties page appears, make the changes you want, then click **Save**.

Deleting a Task

If you no longer want to perform a task, put a check in the box in front of its name and click **Delete** at the top-right of the panel.

Appliance Files

The *Appliance Files* menu is used for two purposes: centralized firmware management, and restoring previously backed up configuration files.

Firmware Files

The Appliance Files menu opens to the *Firmware Files* page.

This page lists all the firmware upgrade files stored on the NetDirector AXS – showing you at a glance the specific information about each of them.

By making the latest firmware upgrade files available for distribution from this single location, you can easily perform upgrades from within the NetDirector AXS, and ensure that all the devices on your installation are operating at the same, most up-to-date, firmware level.

Note: 1. Firmware upgrades are performed under the *Tasks* submenu. See page 133 for details.

2. New firmware upgrade packages are posted on our website as they become available. Check the website regularly to find the latest packages and information relating to them.

Adding Firmware Files

To add a firmware file to the list, do the following:

1. At the top-right of the panel, click **Add** to bring up the *Add Firmware File* page:



2. Browse to the location where the upgrade files that you have downloaded from our website are stored, and select the appropriate file.
3. Provide a description for the file.
4. click **Save** (at the top-right of the main panel) to complete the procedure and add the firmware file to the list.

Note: If the firmware file isn't a NetDirector AXS compliant one (even though it is compliant for the device in a stand-alone configuration), the NetDirector AXS will not let you load it.

Deleting Firmware Files

To remove a firmware file from the list, do the following:

1. Select **Firmware** in the Sidebar.
2. In the Interactive Display panel, click to put a check in front of the file you wish to remove from the list.

Note: You can remove more than one file by checking as many items as you require. You can remove all the files by checking the box at the top of the column.

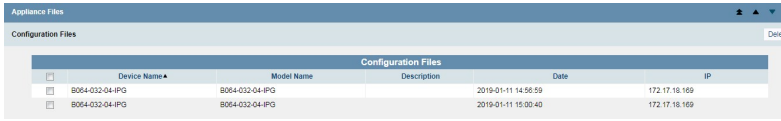
---

3. After you have made your selection, click **Delete** at the top-right of the panel.
4. In the confirmation popup that appears, click **OK**.

Configuration Files

Deleting Configuration Files

Clicking on *Configuration* in the Sidebar brings up the *Configuration Files* page, which looks similar to the screen shown below:



This page lists the backup configurations for the server made with the *Backup device configuration/account information* task (see page141 for details), and allows you to delete the files you no longer wish to keep.

To delete a device's configuration, do the following:

1. Put a check in front of the configuration you want to delete.
2. Click **Delete** (at the top-right of the panel).

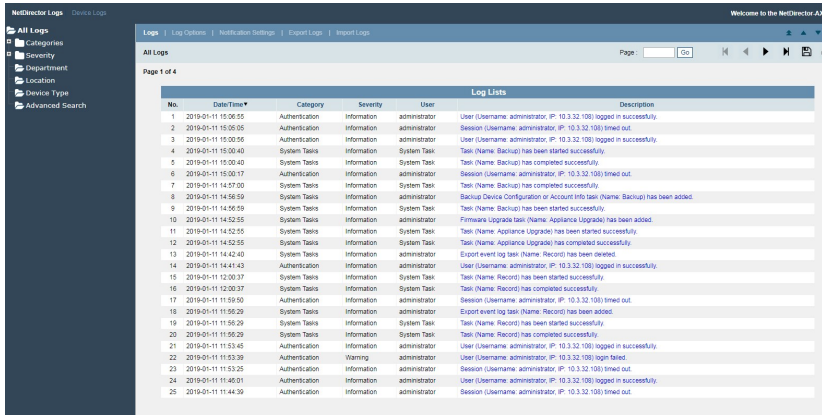
Chapter 8
Logs

Overview

The NetDirectorAXS keeps an extensive record of all the transactions that take place on its installation. The *Logs* page provides a powerful array of filters and functions that allow you to view and export the log file data, as well as be informed by email of specified events as they occur.

NetDirector Logs

When you click the Logs tab, the NetDirectorAXS opens to the default *NetDirector Logs* page which looks similar to the page, below:



- The default layout shows information concerning all of the events that have taken place on all the logs on the entire NetDirectorAXS installation, displayed in reverse chronological order.
- You can change the sorting order of the display by clicking the column headings; You can reverse the order of a selected heading by clicking it a second time.
- The Sidebar provides a filtering function – click an item to only display the events that pertain to it. The last item, *Advanced Search*, is described in detail on page 156.

Note: 1. In general, a blank page, indicates that there were no log events recorded for that category.

2. If the *Device Traps* page (Categories → Device Traps) is blank, however, it may indicate that Event Trap Notification has not been enabled.

- Enter a page number in the *Page* field at the top of the main panel and click *Go* to be taken directly to the selected page.
- The top row of buttons at the upper-right of the main panel navigate through the Sidebar (see *The Navigation Buttons*, page 28).
- The first four buttons on the lower row navigate through the pages of the listed events. The left takes you to the first page; the right takes you to the last page; the middle buttons move you backward or forward one page.

Note: These buttons are only active when there is a relevant action they can perform. For example, when there is more than one page of information and you are on the first page, the "move forward" and "last page" buttons are active, but the "move backward" and "first page" buttons are not.

- Clicking on an item's *Description* brings up a page with detailed information about the item:



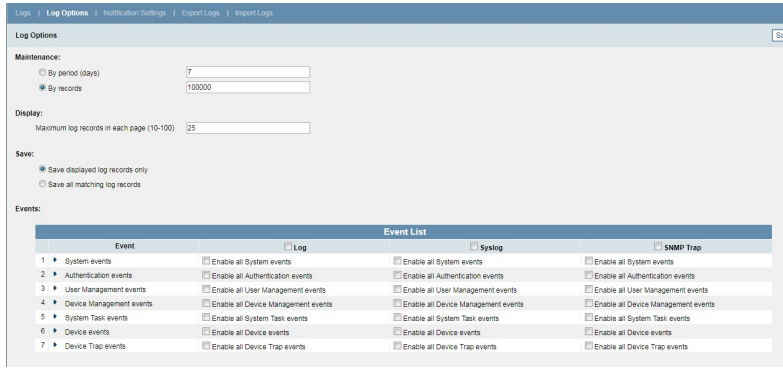
A link in the Device Type Description line also provides more detailed device ID information in a further pop-up window.

Use the buttons at the top-right of the panel to move to the previous or next item in the details view, or close the page and go back to the *Log* page.

- To save the log list to a file, click the button with the diskette icon. (Only the list that is displayed – all, or a filtered choice – is saved).
- To print out the log list, click the button with the printer icon. (Only the list that is displayed – all, or a filtered choice – is printed).

ND Log Options

The *ND Log Options* page gives you control over log file composition and maintenance. When you select **Options**, a page similar to the one below



The meanings of the configuration items are described in the table, below:

Item	Description
Maintenance	Click a radio button to select whether to maintain the log database on a days or records basis, then select the number of days or records to maintain the database for. When the number is reached, events are discarded on a “first in first out” basis. The valid range is from 7–90 days, and 1000–100,000 records.
Display	Sets the maximum number of events to display on the web page. The valid range is from 10–100.
Save	Click a radio button to select whether to save only the events that are displayed, or to save all the events that correspond to the selections made in the Events List (see *Events*, below) when the log file is saved.

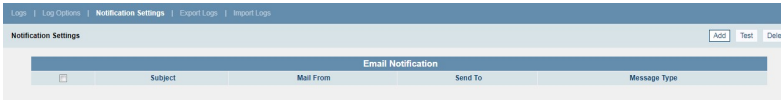
Item	Description
Events	◆ Lets you select which events you want to track, and whether to record them in the ND Log, the Syslog, the SNMP trap, or all. Clicking to put a checkmark in a checkbox enables your choice. ◆ There are 7 event categories; each category contains a list of separate events. To record all of the events for a category, put a checkmark in the checkbox in front of the **Enable all ... events** entry. ◆ To only record selected events for a category (rather than all of them), click the arrowhead in front of the category name to open the list of events; then check or uncheck each event.

Event List

	Event	CC Log	Syslog	Snmp Trap
1	System events	Enable all System events	Enable all System events	Enable all System events
2	Authentication events	Enable all Authentication events	Enable all Authentication events	Enable all Authentication ever
3	User Management events	Enable all User Management events	Enable all User Management events	Enable all User Management events
4	Device Management events	Enable all Device Management events	Enable all Device Management events	Enable all Device Manageme events
5	System Task events	Enable all System Task events	Enable all System Task events	Enable all System Task event
6	Device events	Enable all Device events	Enable all Device events	Enable all Device events
7	Device Trap events	Enable all Device Trap events	Enable all Device Trap events	Enable all Device Trap events

Notification Settings

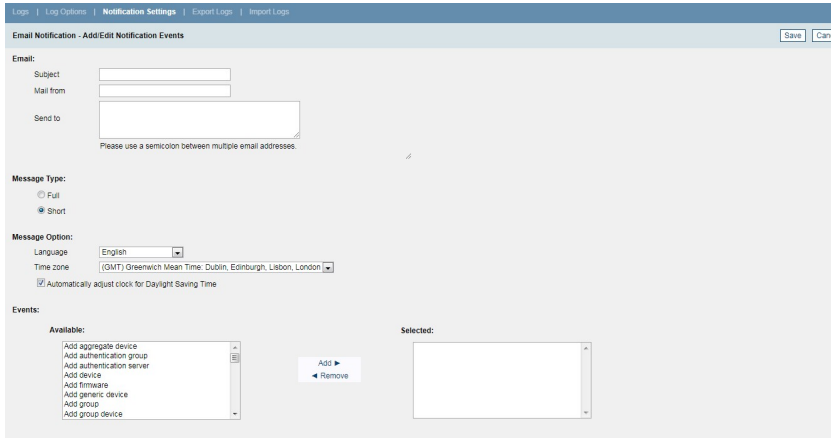
The *Notification Settings* page is used to inform a specified user of specified events that occur on the NetDirectorAXS installation. When you select **Notification Settings**, a page similar to the one below appears:



Adding and Configuring Notification Users

To add users and specify the events they will receive notification of, do the following:

1. Click Add at the top-right of the panel. The *Email Notification - Add/Edit Notification Events* page appears:



2. Key an appropriate title for the notification message in the *Subject* field
3. Key in the email address of one of the administrators in the *Mail from* field.
4. Key in the email address of the person who will receive the email notification in the *Send to* field. If you want the notification to go to more than one person, use a semicolon to separate the email addresses. There should not be a space before or after the semicolon.
5. Select whether the message type will be *Full* or *Short*.
6. Select an event that you want to receive email notification of in the *Available* column, then click **Add** to move it into the *Selected* column. Repeat for any other events you want to receive email notification of.
7. When you have finished filling out this page, click **Save** to save the configuration and return to the *Notification Settings* page.

Modifying Notification Configurations

To modify a notification configuration, click its *Subject* name in the *Email Notification* table; make your desired changes on the *Email Notification - Add/ Edit Notification Events* page; and click **Save** at the top-right of the panel.

Deleting Notification Configurations

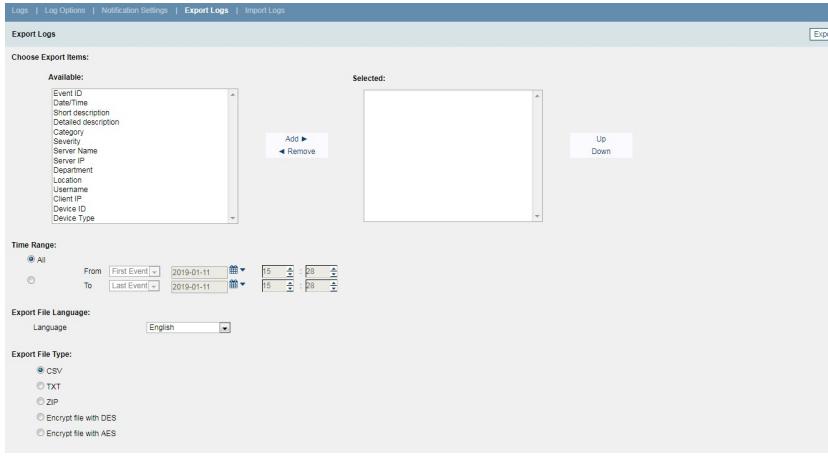
To delete a notification configuration, click to put a check in the checkbox in front of its *Subject* name in the *Email Notification* table; then click **Delete** at the top-right of the panel.

Testing Event Notifications

To check that an event notification is working properly, click to put a check in the checkbox in front of the notification's *Subject* name in the *Email Notification* table, then click **Test**. If the system is working properly, the event notification recipient will receive an email with the event notification.

Export Logs

The *Export Logs* page is used to save specified logged events to a file. When you select *Export Logs* on the Submenu bar, a page similar to the one below appears:



To save specified logged events to a file, do the following:

1. Select a log file item that you want to include in the exported file in the *Available* column, then click **Add** to move it into the *Selected* column. Repeat for any other log file items you want to include.
2. To change the order of the *Selected* items, click on the item you want to move, then click **Up** or **Down** to change it to the position you want.
3. For *Time Range*, selecting **All** exports all the records that exist in the database for the selected items. To export records for a particular time period, select the radio button below it and set the time parameters with the *From* and *To* settings.
4. For *Export File Language*, choose **Default** to have the file exported in the language that your browser is set to. If you prefer a different language, drop down the list and select one of the languages offered.
5. For *Export File Type*, click the radio button in front of your choice. If you choose one of the encryption options, key a password into the *Password* field that comes up.

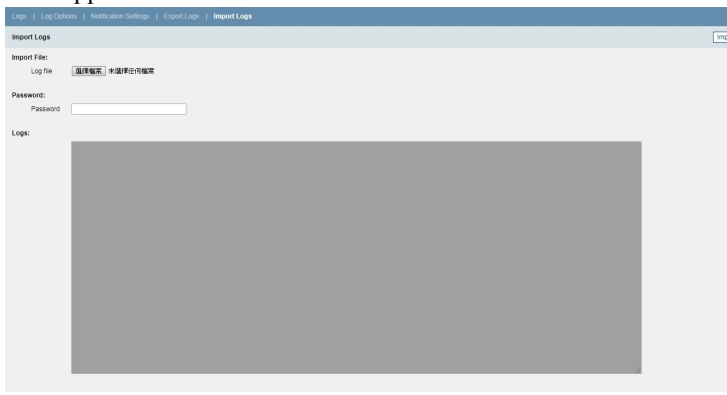
   Note: Make a note of the password – you will need it to import the file (see Import File in the next section).

6. When you have finished making your choices, click **Export** (at the top-right of the panel).
7. In the dialog box that comes up, select the “save file” option. The log file is saved in the location you specify.

   Note: You can rename the files to anything you like, as long as you don’t change the extension.

Import Logs

The *Import Logs* page is used to open previously saved log files for viewing. When you select *Import Logs* on the Submenu bar, a page similar to the one below appears:



To import a previously saved log file, do the following:

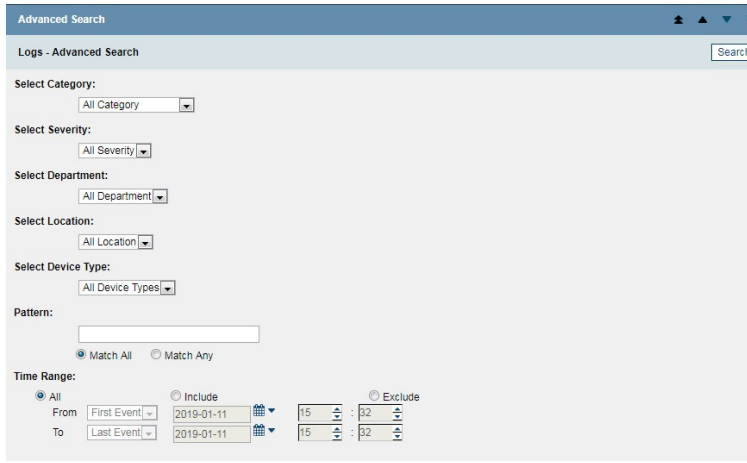
1. Either key in the full path to the file in the *Log file* field, or click **Browse** to navigate to it.
2. If the file has been encrypted, key the password that was used when it was created into the *Password* field.
3. Click **Import** (at the top-right of the panel).

When the file is imported, its contents appear in the *ND Log List* panel.

Advanced Search

Advanced Search lets you very finely tune your search by narrowing down the parameters for each of the search choices. To perform an advanced search, do the following:

1. In the Sidebar, click **Advanced Search**. A screen, similar to the one below appears:



2. Drop down each of the lists you want to select specific search parameters.
3. If you want to search for a particular word or string, key it in the *Pattern* field, then select whether all or any of the terms are required for a match.
4. For *Time Range*, selecting **All** searches all the records that exist in the database. To search for a particular time period, click *Include* or *Exclude*, and set the time parameters with the *From* and *To* settings.

Note: 1. If *Include* is selected, all the events that fall within the specified time range are searched.

2. If *Exclude* is selected, only the events that fall outside of the specified time range are searched.

---

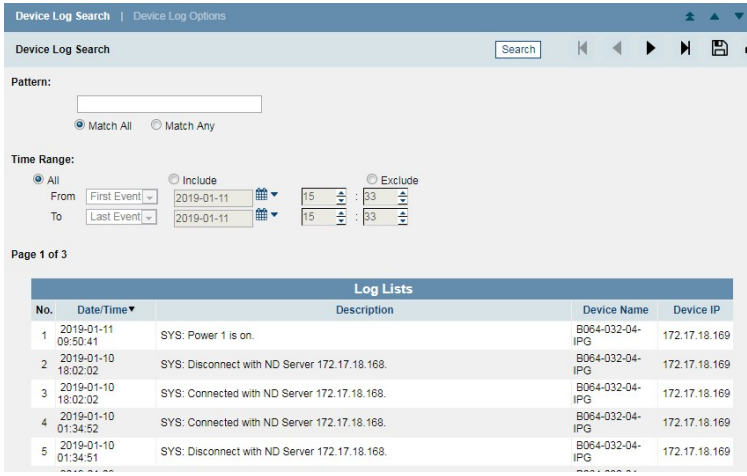
5. When you have finished making your choices, click **Search** (at the top-right of the panel).

The search results are displayed in the Log List in the main panel.

- To save the search results to a file, click the button with the diskette icon.
- To print out the search results, click the button with the printer icon.
- The sort order of the list can be changed by clicking the column headings.

Device Logs

The NetDirector AXS acts as a log server for all Tripp Lite over IP KVM switches,recording the system events that take place on those devices in a database. When you click *Device Logs* on the Submenu bar, the *Device Logs Search* page, which allows you to search for events containing specific words or strings, appears:



- The default layout shows log information for all of the devices on the entire NetDirector AXS installation displayed in reverse chronological order.
  - Clicking the *Date/Time* column heading changes the sorting order between standard and reverse chronological order.
  - Clicking the *Description* column heading changes the sorting order between standard and reverse alphabetical order.
- The Sidebar provides a filtering function – click a device to only display the events that pertain to it.
- The navigation buttons (arrowheads) at the top-right of the main panel move you through the pages of the log list. The leftmost takes you to the first page; the rightmost takes you to the last page; the middle buttons move you backward or forward one page.

Note: These buttons are only active when there is a relevant action they can perform. For example, when there is more than one page of information and you are on the first page, the “move forward one page” and “move to the last page” buttons are active, but the “move backward one page” and “move to the first page” buttons are not.

- To save the log list to a file, click the button with the diskette icon. (Only the list that is displayed – all, or a filtered choice – is saved).
- To print out the log list, click the button with the printer icon. (Only the list that is displayed – all, or a filtered choice – is printed).

Device Log Search

To search the logs, do the following:

1. If you want to search for a particular word or string, key it in the *Pattern* field.
2. Use *Match All* for a search that must contain all words in the *Pattern* field; or *Match Any* for a search which can contain any or all words in the *Pattern* field.
3. For *Time Range*, selecting **All** searches all the records that exist in the database for the selected pattern. To search records for a particular time period, select either the *Include* or *Exclude* radio button, and set the time parameters with the *From* and *To* settings.

Note: 1. If the *Include* button is selected, all the events that fall within the specified time range are searched.

2. If the *Exclude* button is selected, only the events that fall outside of the specified time range are searched.

---

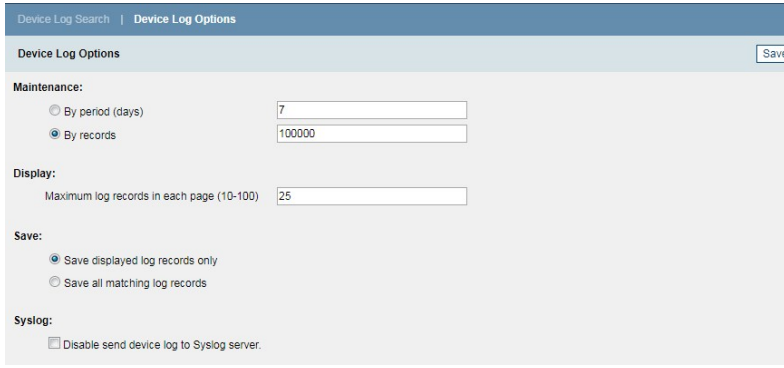
4. When you have finished making your choices, click **Search** (at the top-right of the panel).

The search results are displayed in the Log List in the main panel.

- To save the search results to a file, click the button with the diskette icon.
- To print out the search results, click the button with the printer icon.
- The sort order of the list can be changed by clicking the column headings.

Device Log Options

The *Device Log Options* page provides management options regarding the NetDirector AXS' device log database. When you select *Device Log Options*, a page similar to the one below appears:



- **Maintenance** allows you to select whether to maintain the device log database on a days or records basis. Click a radio button to make your selection, then key in the number of days or records to maintain the database for. When the number is reached, events are discarded on a "first in first out" basis.
- **Display** allows you to set the maximum number of record events to display on the web page.
- **Save** allows you to save the device logs to a file:

  1. First click a radio button to choose whether to save only the currently selected device log records, or all of the device log records, then click **Save** (at the top-right of the panel).
  2. In the dialog box that comes up, select the "save file" option. The log file is saved in CSV format, which can be read by a spreadsheet program.

Appendix A
Technical Information

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **https://www.tripplite.com/support/help**
- For telephone support, see *Telephone Support*, page iii.

North America

Email Support		techsupport@tripplite.com
Online Technical Support	Troubleshooting Documentation Software Updates	https://www.tripplite.com/support/help
Telephone Support		1.773.869.1234

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

Supported KVM Switches

The following is a list of fully supported KVM switches that can be used in a cascaded installation.

- B064 series (B064-016-02-IPG, B064-032-02-IPG, B064-016-04-IPG and B064-032-04-IPG), please check website for compatible KVM switches.

Note: The installation cannot be cascaded beyond the second level.

Device ANMS Settings

To enable ND Management of a device from the device's ANMS settings page, do the following:

1. Log into the device.
2. Refer to the device's User Manual to locate its ANMS settings page.
3. In the ANMS page, click the checkbox to *enable* ND Management, then key in the IP address and device port number (see *Device port*, page 15), of the NetDirector AXS server that will manage the device.

VPNs

Basically, a VPN (virtual private network) is a private network that uses a public network (usually the Internet) to connect several sites together. It typically includes several WANs. Many companies create their own VPN to provide a secure network connection between two sites. One drawback to VPNs, however, is that while the network is secure, throughput can be slow.

Firewalls

When NetDirector AXS servers is located behind firewall, the following service ports must be specified on the server, and the corresponding ports must be opened on the firewall.

1. ND Port

Note: Each NetDirector AXS server can have a different setting. But the port opened on the firewall must correspond to the ND Port setting

---

2. The NetDirector AXS server's HTTPS port
3. The NetDirector AXS Proxy port (see NetDirector AXS *Proxy Function* in the next section).

Note: You can open this port if you would like NetDirector AXS Client Workstations outside the firewall to be able to directlyopen a web browser session to the Secondary server inside the firewall.

NetDirector AXS Proxy Function

The NetDirector AXS Proxy function relates to NetDirector AXS servers located behind a firewall. For NetDirector AXS ClientWorkstations that are outside the firewall to access KVM devices managed by NetDirector AXS server inside the firewall, the Proxy function must be enabled on that server, and the port specified as the proxy port must be opened on the firewall.

Note: 1. While a NetDirector AXS Client Workstation outside the firewall can open a web browser session with a NetDirector AXS server inside the firewall when the proxy port hasn't been specified and opened, viewers for the KVM devices managed by that NetDirector AXS server cannot be opened.

2. If the Proxy function isn't enabled, and you still want to access the devices, you must open all the service ports (HTTPS, Program, Virtual Media, Telnet, SSH, etc.) on the firewall required by the devices.

Name, Description and Range Parameters

The following table lists the parameters and defaults for names, descriptions and ranges found in the NetDirector AXS system:

Note: Unless otherwise specified, field entries can be input in any supported language.

Category		Length / Range	Default
Users	Login name	Up to the equivalent of 16 English alphanumeric characters. The minimum number is based on the account policy settings (see *NetDirector AXS Authentication*, page 72). The following characters may not be used: **/ \ [ ] : ; | = , + * ? < > @ " '**	
	Screen name	Up to 32 Bytes. The following characters may not be used: **" '**	
	Password	The equivalent of 0–16 English alphanumeric characters. The minimum number is based on the account policy settings (see *NetDirector AXS Authentication*, page 72). 0 means no password authentication.	
	Description	Up to 256 Bytes.	
	Session Timeout	1–99 min.	3 min
	Unexpected disconnection timeout	2–10 min.	2 min.
	Email	Up to 256 Bytes. **From:** 0–64 **To:** 0–128 **Subject:** 1–128	
Groups	Name	2–32 Bytes. The following characters may not be used: **" '**	
	Description	Up to 256 Bytes.	

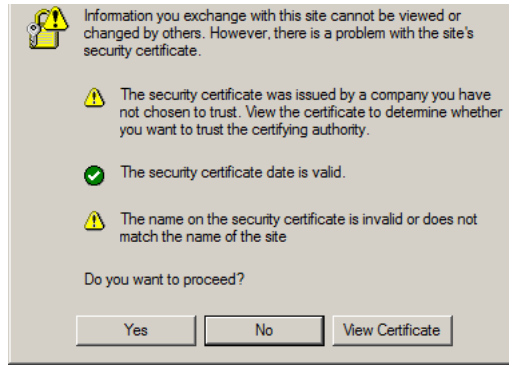
Category		Length / Range	Default
User Types	Name	2–32 Bytes. The following characters may not be used: **" '**	
	Description	Up to 256 Bytes.	
Authentication Server	Server name	2–32 Bytes. The following characters may not be used: **" '**	
	Description	Up to 256 Bytes.	
	Browser Method	Unlimited for Username and Password. **Note:** NetDirector AXS performance is adversely affected if there are too many characters.	
NetDirector AXS Authentication	Username Minimum	Up to the equivalent of 16 English alphanumeric characters. The minimum number is based on the account policy settings (see *NetDirector AXS Authentication*, page 72). The following characters may not be used: **/ \ [ ] : ; | = , + * ? < > @ " '**	6
	Password Minimum	The equivalent of 0–16 English alphanumeric characters. The minimum number is based on the account policy settings (see *NetDirector AXS Authentication*, page 72). 0 means no password authentication.	6
	Password Expires	No limit on the number of days.	
Devices	Name	0–32 Bytes.	
	Description	Up to 256 Bytes.	
	Contact name	No limit on the number of Bytes.	
	Telephone	No limit on the number of Bytes.	
	Email notification	No limit on the number of Bytes.	
Aggregate Devices	Name	1–32 Bytes.	
	Description	Up to 256 Bytes.	
Folders	Name	1–32 Bytes.	
	Description	Up to 256 Bytes.	
Departments / Locations	Name	1–32 Bytes.	
	Description	Up to 256 Bytes.	

Category		Length / Range	Default
Tasks	All Tasknames	No limit on the number of Bytes.	
	Database Backup Password	0–8 Bytes. 0 means no password authentication.	
	Export Device Log Pattern	No limit on the number of Bytes.	
ND Log Options	By Period	7–90 days	
	By Record	1000–100,000	
	Records per page	10–100	
Log Notification Settings	Subject	1–128 Bytes.	
	Mail from	Up to 64 Bytes.	
	Send to	Up to 128 Bytes.	
Preferences: Web Options	Display screen name	0–32 Bytes.	

Trusted Certificates

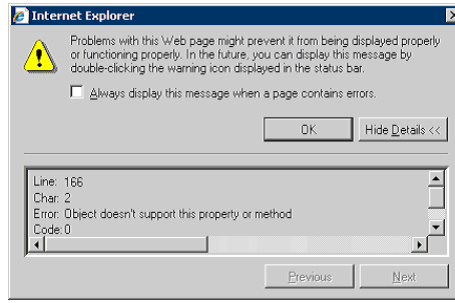
Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.



The certificate can be trusted, but the alert is triggered because the certificate's name is not found on the Microsoft list of Trusted Authorities. You can ignore the warning and click **Yes** to go on.

Note: To avoid users having to go through the certificate acceptance prompt each time they log in, you can use athird party certificate authority (CA) to obtain a signed certificate. See *Importing a Signed SSL Server Certificate*, page 132, for details.



1. Reset the Internet Explorer security settings to enable Active Scripting, ActiveX controls, and Java applets

   By default, Internet Explorer 6 and some versions of Internet Explorer 5.x use the High security level for the Restricted sites zone and Microsoft Windows Server 2003 uses the High security level for both the Restricted sites zone and the Internet zone. You may want to enable Active Scripting, ActiveX controls, and Java applets. To enable Active Scripting, ActiveX controls, and Java applets, follow these steps:

   a) Start Internet Explorer.

   b) On the Tools menu, click Internet Options.

   c) In the Internet Options dialog box, click Security.

   d) Click Default Level.

   e) Click OK.

2. Verify that Active Scripting, ActiveX, and Java are not blocked

   If some computers work but other, verify that Internet Explorer or another program on your computer such as an anti-virus program or a firewall are not configured to block scripts, ActiveX controls, or Java applets.

3. Verify that your anti-virus program is not set to scan the Temporary Internet Files or Downloaded Program Files folders

4. Delete all the temporary Internet-related files

   To remove all the temporary Internet-related files from your computer, follow these steps:

   a) Start Internet Explorer.

   b) On the Tools menu, click Internet Options.

   c) Click the General tab.

   d) Under Temporary Internet files, click Settings.

   e) Click Delete Files.

   f) Click OK.

   g) Click Delete Cookies.

   h) Click OK.

   i) Under History, click Clear History, and then click Yes.

   j) Click OK.

5. Make sure that you have the latest version of Microsoft DirectX installed

   For information about how to install the latest version of Microsoft DirectX, visit the following Microsoft Web site:

   http://www.microsoft.com/windows/directx/default.aspx?url=/windows/directx/downloads/default.htm

6. Make sure that you have the latest version of the Java JRE installed.

   For information about how to install the latest version of the JRE visit the Java Web site: www.java.com

Note: The ND Viewer does not support OpenJDK.